JOURNAL OF NUMBER THEORY **20**, 1–69 (1985)

Linear Forms in Elliptic Logarithms

KUNRUI YU

Institute of Mathematics, Academia Sinica, Beijing, The People's Republic of China

Communicated by M. Waldschmidt

Received February 11, 1983

New lower bounds for linear forms in n ($\geqslant 2$) elliptic logarithms in the CM case are established. The estimate is better than all previous estimates with respect to some of the parameters that appear. It may be interesting to notice that the product $\log A_1 \cdots \log A_n$ in the lower bound (see the Corollary of Theorem 1) is of exactly the same form as in the lower bounds for linear forms in logarithms of algebraic numbers (see A. Baker [*in* "Transcendence Theory: Advances and Applications." (A. Baker and D. W. Masser, Eds.), pp. 1–27, Academic Press, New York, 1977]) and this is the first time such a parallelism has been achieved. To obtain the above lower bounds a zero estimate on the group variety $G_a^n \times E$ ($\mathbb{C}^n \times E$) is established (with E being an elliptic curve with CM), which is sharper than that derived from the general results in D. W. Masser and G. Wüstholz (*Inventiones Math.* **63** (1981), 81–95).

1. INTRODUCTION AND RESULTS

Let $\wp(z)$ be a Weierstrass elliptic function determined by the differential equation

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2\wp(z) - g_3, \tag{1.1}$$

where g_2, g_3 are algebraic numbers with $g_2^3 \neq 27g_3^2$. Let E be the elliptic curve defined by the equation

$$y^2 = 4x^3 - g_2x - g_3. \tag{1.2}$$

We parameterize E as

$$x = \wp(z), \qquad y = \wp'(z) \tag{1.3}$$

and write $p = p(z) = (\wp(z), \wp'(z))$, where the parameter z ranges over all complex numbers not lying on the period lattice $\mathscr{L}$ of $\wp(z)$. We can view E as a group variety whose origin O is the point at infinity.

0022-314X/85 $3.00

We now define

$$\Lambda_1 = \beta_0 + \beta_1 u_1 + \cdots + \beta_n u_n,$$

where $\beta_0, \ldots, \beta_n$ are algebraic numbers, not all zero, and $u_1, \ldots, u_n$ are algebraic points of $\wp(z)$; by an algebraic point of $\wp(z)$ we mean a number $u \in \mathbb{C}$ (the field of complex numbers) such that either $\wp(u)$ is algebraic or u is a pole of $\wp(z)$. Siegel proved in 1932 that there exists $u_1 \in \mathscr{L}$ such that $\Lambda_1 \neq 0$. Schneider proved in 1937 that $\Lambda_1 \neq 0$ when $n = 1$, $u_1 \neq 0$, and $n = 2$, $\beta_0 = 0$, $u_1 \neq 0$, $u_2 \neq 0$, provided that $\wp(u_1 z)$ and $\wp(u_2 z)$ are algebraically independent. In 1968, Baker [4] proved that $\Lambda_1 \neq 0$ when $n = 2$, $\beta_0 \neq 0$, and u_1, u_2 are fundamental periods of $\wp(z)$. In 1975, Masser [19] showed that $\Lambda_1 \neq 0$ in the case when $\wp(z)$ has complex multiplication and $u_1, \ldots, u_n$ are linearly independent over the corresponding complex quadratic field k. Subsequently Coates, Lang, and Anderson have given quantitative refinements of this result; see Anderson [1, 2]. See also Groscot [12] when g_2, g_3 are rational integers divisible by 4. The estimates are somewhat weaker than those established in the case of linear forms in logarithms. Their methods extended Baker's [5] method by utilizing Bashmakov's [6] result concerning the Galois group of division points of $\wp(z)$ (see also Lang's book [16]). We simply call these methods Baker's method.

In 1980, Bertrand and Masser [8], by means of the Schneider–Lang theorem, proved that $\Lambda_1 \neq 0$ in the case when $\wp(z)$ has no complex multiplication and $u_1, \ldots, u_n$ are linearly independent over the field $\mathbb{Q}$ of rational numbers. Their method can be extended to furnish a new proof of Masser's theorem, stated in the preceding paragraph, and adapted to yield quantitative results, but these are weak compared with the lower bounds obtained by Baker's method.

Our primary purpose in this paper is to prove a new lower bound for $|\Lambda_1|$ with $\beta_0 = 0$ and $n \geqslant 2$, i.e., for $|\Lambda|$, where

$$\Lambda = \beta_1 u_1 + \cdots + \beta_n u_n \qquad \text{with} \quad n \geqslant 2,$$

assuming that $\wp(z)$ has complex multiplication over the complex quadratic field k. (Henceforth we will always keep this assumption.) Let K be a number field of degree D over $\mathbb{Q}$ containing the field k and the numbers $g_2, g_3, \beta_1, \ldots, \beta_n$, $\wp(u_i)$, $\wp'(u_i)$ with $1 \leqslant i \leqslant n$ and $u_i \notin \mathscr{L}$. We use the logarithmic absolute height $h(\alpha)$ for $\alpha \in \bar{\mathbb{Q}}$ (the field of all algebraic numbers) and $h(p)$ on the elliptic curve E (for the details see Sect. 2 below). We suppose that $\beta_1, \ldots, \beta_n$ are linearly independent over k and $u_i \neq 0$ $(1 \leqslant i \leqslant n)$. For each i with $1 \leqslant i \leqslant n$, let $p_i = p(u_i)$ if $u_i \notin \mathscr{L}$ and let $p_i = O$ (the point at infinity) if $u_i \in \mathscr{L}$. Suppose that V_i, V, Y, W are positive numbers satisfying

$$V_i \geqslant \max(1, h(p_i), |u_i|^2/D) \qquad (1 \leqslant i \leqslant n),$$

$$V = \max_{1 \leqslant i \leqslant n} V_i,$$

$$1 \leqslant Y \leqslant \min_{1 \leqslant i \leqslant n} \log(eDV_i/|u_i|^2),$$

$$W = \max_{1 \leqslant i \leqslant n} h(\beta_i).$$

Then we have

THEOREM 1. *There exists a constant $c > 0$ depending effectively on n and E such that*

$$|\Lambda| > \exp(-cD^{n^2} V_1 \cdots V_n (W + \log(DV) + Y)^{n(n-1)} Y^{1-n^2}).$$

The meaning of dependence on E of a constant will be clarified at the end of Section 2.

Moreover, if we suppose that

$$u_i \in \Pi = \{t_1\omega_1 + t_2\omega_2 \mid 0 \leqslant t_2, t_2 < 1\} \qquad (1 \leqslant i \leqslant n),$$

where ω_1, ω_2 is a fixed fundamental pair of periods of $\wp(z)$, and let A_i $(1 \leqslant i \leqslant n)$, B be positive numbers such that

$$A_i \geqslant \max(H(\wp(u_i)), e^e) \qquad (1 \leqslant i \leqslant n),$$

$$A_1 \leqslant A_2 \leqslant \cdots \leqslant A_n,$$

$$B \geqslant \max(H(\beta_1), \ldots, H(\beta_n), e),$$

where $H(\alpha)$ denotes the usual height of algebraic number α (i.e., the maximum of the absolute values of the coefficients of its minimal polynomial over $\mathbb{Z}$, the ring of rational integers), then Theorem 1 has the following

COROLLARY. *There exists a constant $c_1 > 0$ depending effectively on n and E such that*

$$|\Lambda| > \exp\{-c_1 D^{n^2} \log A_1 \cdots \log A_n (\log B + \log\log A_n)^{n(n-1)} (\log\log A_1)^{1-n^2}\}. \quad (1.4)$$

The previously best known result, due to Anderson [2, Theorem IV], states that

$$|\Lambda| > \exp\{-c_1' D^{n^2+4n+6+\varepsilon} (\log A_{n-1})^{n^2+n-2+\varepsilon} \log A_n \cdot (\log B + \log\log A_n) \cdot (\log\log(B \log A_n))^{n+2+\varepsilon}\},$$

where c_1' depends effectively on n, E, and the arbitrarily chosen $\varepsilon > 0$. Our lower bound (1.4) is usually much stronger in its dependence on $A_1,\ldots,A_n$ except when A_n is much larger than A_{n-1}; it is stronger in its dependence on D, but weaker in its dependence on B. It may be interesting to notice that the product $\log A_1 \cdots \log A_n$ in (1.4) is of exactly the same form as in the lower bounds for linear forms in logarithms of algebraic numbers (see Baker [5]), and this is the first time such a parallelism has been achieved. We remark further that Theorem 1 implies Masser's important theorem (stated in the second paragraph above) in the case when $\beta_0 = 0$ by some simple argument from linear algebra. We have thus given the third proof of that theorem (with $\beta_0 = 0$). We remark also that in the case when $n = 2$ the hypothesis of Theorem 1 and the Corollary on the linear independence (over k) of $\beta_1,\ldots,\beta_n$ can be relaxed to that of assuming $\Lambda \neq 0$ (see the author's forthcoming paper [29]) and that a result of this type (with respect to $A_1,\ldots,A_n$) for $n = 2$ was claimed by G. V. Chudnovsky in his address on ICM, Helsinki, 1978 (see [11]).

Our secondary purpose is to prove a result on the linear dependence of algebraic points of $\wp(z)$. Let $u_1,\ldots,u_n$ $(n \geqslant 2)$ be algebraic points of $\wp(z)$, D and V_i $(1 \leqslant i \leqslant n)$ be positive numbers such that

$$D \geqslant \max(3, [k(g_2, g_3, \wp(u_i), \wp'(u_i): 1 \leqslant i \leqslant n, u_i \notin \mathscr{L}): k(g_2, g_3)])$$

$$V_i \geqslant \max(1, h(p_i), |u_i|^2/D),$$

where $p_i = p(u_i)$ if $u_i \notin \mathscr{L}$ and $p_i = O$ if $u_i \in \mathscr{L}$. Denote by $\mathscr{O}$ the ring of endomorphisms of $\mathscr{L}$ (see Section 2 for details). Then we have

THEOREM 2. *Suppose that $u_1,\ldots,u_n$ are linearly dependent over k. Then there exist $\sigma_1,\ldots,\sigma_n$ in $\mathscr{O}$, not all zero, and a constant $c_2 > 0$ depending effectively on E, such that*

$$\sigma_1 u_1 + \cdots + \sigma_n u_n = 0$$

and

$$|\sigma_i|^2 \leqslant (c_2(n-1)^2 D^3 (\log D)^2)^{n-1} V_1 \cdots V_n / V_i \qquad (1 \leqslant i \leqslant n).$$

Furthermore, if we suppose that

$$0 \neq u_i \in \Pi \qquad (1 \leqslant i \leqslant n),$$

and let A_i $(1 \leqslant i \leqslant n)$ and D be positive numbers such that

$$A_i \geqslant \max(H(\wp(u_i)), e),$$

$$D \geqslant \max(e^e, [k(g_2, g_3, \wp(u_i), \wp'(u_i): 1 \leqslant i \leqslant n): k(g_2, g_3)]),$$

then we have

THEOREM 2′. *Suppose that $u_1,\dots,u_n$ are linearly dependent over k. Then there exist $\sigma_1,\dots,\sigma_n$ in $\mathcal{O}$, not all zero, and a constant $c_2'>0$ depending effectively on E, such that*

$$\sigma_1 u_1+\cdots+\sigma_n u_n=0$$

and

$$|\sigma_i|^2\leqslant (c_2'(n-1)^2D^2(\log D)^2)^{n-1}\log A_1\cdots\log A_n/\log A_i \quad (1\leqslant i\leqslant n).$$

Note that Theorems 2 and 2′ improve Anderson [2, Theorem II]. By virtue of Theorem 2, it is not difficult to see that we may assume that in Theorem 1 $u_1,\dots,u_n$ are linearly independent over k; in other words, Theorem 1 is a consequence of Theorem 1′, given below (we will deduce Theorem 1 from Theorem 1′ later on, in Sect. 8). For $n\geqslant 1$, let $u_0,u_1,\dots,u_n$ be algebraic points of $\wp(z)$ which are linearly independent over k and $\beta_1,\dots,\beta_n$ be algebraic numbers such that $1,\beta_1,\dots,\beta_n$ are linearly independent over k. Suppose that K is a number field of degree D over $\mathbb{Q}$ containing the field k and the numbers $g_2, g_3, \beta_1,\dots,\beta_n$, $\wp(u_i)$, $\wp'(u_i)$ with $0\leqslant i\leqslant n$, $u_i\notin\mathscr{L}$. For $0\leqslant i\leqslant n$, put $p_i=p(u_i)$ if $u_i\notin\mathscr{L}$ and $p_i=O$ if $u_i\in\mathscr{L}$. Suppose that

$$V_i\geqslant \max(1,h(p_i),|u_i|^2/D) \qquad (0\leqslant i\leqslant n),$$

$$V=\max_{0\leqslant i\leqslant n} V_i,$$

$$1\leqslant Z\leqslant \min_{0\leqslant i\leqslant n}\min(DV_i,\log(eDV_i/|u_i|^2)), \tag{1.5}$$

$$W\geqslant \max_{1\leqslant i\leqslant n} h(\beta_i),$$

$$J=W+\log(DV),$$

$$V_0\geqslant |\beta_i|^2 V_i \qquad (1\leqslant i\leqslant n). \tag{1.6}$$

Write $\Lambda=\beta_1u_1+\cdots+\beta_nu_n-u_0$.

THEOREM 1′. *There exists a constant $c'>0$ depending effectively on n and E such that*

$$|\Lambda|>\exp(-c'D^{(n+1)^2}V_0\cdots V_n(J+Z)^{n(n+1)}Z^{-n(n+2)}).$$

The main part of the present paper is devoted to the proof of Theorem 1′. The proof is divided into analytic and algebraic parts. The analytic part uses Waldschmidt's [26] powerful interpolation method in several variables (see Lemma 2.13 below). Following some general ideas of Nesterenko, Brow-

nawell and Masser [10], Masser [21], and especially of Masser and Wüstholz [22], with some modification, we prove a zero estimate on the group variety $G_a^n \times E$ ($\mathbb{C}^n \times E$) which is sharper than that derived from the general results established in [22], thereby completing the algebraic part.

2. Preliminaries for Analytic Part

Let α be an algebraic number of degree $d \geqslant 1$, $H(\alpha)$ be its height, $a_0 > 0$ be the leading coefficient of its minimal polynomial over $\mathbb{Z}$, $\alpha_1, \ldots, \alpha_d$ be its conjugates. Write

$$M(\alpha) = a_0 \prod_{i=1}^{d} \max(1, |\alpha_i|).$$

Let F be a number field containing α. We write

$$H_F(\alpha) = \prod_v \max(1, |\alpha|_v),$$

where v runs over all valuations of F normalized in the usual way to satisfy the product formula $\prod_v |\alpha|_v = 1$ for $\alpha \neq 0$. More precisely, for each embedding σ of F into $\mathbb{C}$ there is an archimedean valuation v defined by $|\alpha|_v = |\sigma(\alpha)|$, and for each prime ideal $\mathfrak{p}$ of F with absolute norm $N\mathfrak{p}$ there is a non-archimedean valuation v defined by $|\alpha|_v = (N\mathfrak{p})^{-m}$, where $\mathfrak{p}^m$ is the exact power of $\mathfrak{p}$ in the fractional principal ideal of F generated by α. Clearly

$$|\alpha| \leqslant H_F(\alpha). \tag{2.1}$$

The number

$$h(\alpha) = \frac{1}{[F:\mathbb{Q}]} \log H_F(\alpha)$$

is independent of F, and we shall call $h(\alpha)$ the logarithmic absolute height of α. The relation

$$M(\alpha) = H_{\mathbb{Q}(\alpha)}(\alpha)$$

(see, for example, Bertrand [7, Lemma 11]) shows that

$$h(\alpha) = \frac{1}{d} \log M(\alpha).$$

For any algebraic numbers $\alpha, \beta, \alpha_1, \ldots, \alpha_n$ and any $0 \neq m \in \mathbb{Z}$, we have

$$h(\alpha\beta) \leqslant h(\alpha) + h(\beta), \tag{2.2}$$

$$h(\alpha^m) = |m|\, h(\alpha), \tag{2.3}$$

$$h(\alpha_1 + \cdots + \alpha_n) \leqslant h(\alpha_1) + \cdots + h(\alpha_n) + \log n. \tag{2.4}$$

From the inequality

$$M(\alpha) \leqslant (d+1)^{1/2} H(\alpha)$$

(see Mahler [18]) it follows that

$$h(\alpha) \leqslant \frac{1}{d} (\log H(\alpha) + \log d) \tag{2.5}$$

since $h(\alpha) = \log H(\alpha)$ for $\alpha \in \mathbb{Q}$ and $x + 1 \leqslant x^2$ for $x \geqslant 2$.

We now quote a refined Liouville inequality. Denote by $L(Q)$ the length of a polynomial Q, i.e., the sum of the absolute values of its coefficients.

LEMMA 2.1 (Mignotte and Waldschmidt [24]). *Let $\theta_1, \ldots, \theta_r$ be algebraic numbers in a number field of degree d. Let Q be a polynomial in $\mathbb{Z}[x_1, \ldots, x_r]$ having degree at most N_i in x_i $(1 \leqslant i \leqslant r)$. If $Q(\theta_1, \ldots, \theta_r) \neq 0$, then*

$$|Q(\theta_1, \ldots, \theta_r)| \geqslant (L(Q))^{1-d} \exp\left(-d \sum_{i=1}^{r} N_i h(\theta_i)\right).$$

Proof. See [24].

Denote by $\mathcal{O}$ the ring of endomorphisms of the period lattice $\mathcal{L}$ of $\wp(z)$; that is, the ring of complex numbers ρ such that $\rho\mathcal{L} \subseteq \mathcal{L}$. It is well known that $\mathcal{O}$ is a subring of finite index in the ring of algebraic integers of the field k. Henceforth we fix a fundamental pair ω_1, ω_2 of periods of $\wp(z)$ such that $\mathrm{Im}(\omega_2/\omega_1) > 0$. Let a be the least natural number such that $a\omega_2/\omega_1 \in \mathcal{O}$. Fix $\tau = a\omega_2/\omega_1$. It is easily seen that $\mathcal{O}$ can be expressed in the form

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\tau.$$

The elliptic curve E defined by (1.2) becomes a group variety after parameterizing by (1.3), and adding the point at infinity (denoted by O). It inherits the usual law of addition on $\mathbb{C}$. An algebraic point p on E is either the point at infinity O or a point on (1.2) with algebraic coordinates x, y. If F is any subfield of $\mathbb{C}$ containing the field $k(g_2, g_3)$, we write $E(F)$ for the set consisting of all p on E with coordinates in F, together with O. For $\rho \in \mathcal{O}$, $z \in \mathbb{C} \backslash \mathcal{L}$, we define $\rho O = O$, $\rho p(z) = p(\rho z)$ if $\rho z \notin \mathcal{L}$, and $\rho p(z) = O$ if $\rho z \in \mathcal{L}$.

LEMMA 2.2 (Anderson [2]). *For any non-zero $\rho \in \mathcal{O}$ there exist polynomials $A_\rho(x)$, $B_\rho(x)$ in $k(g_2, g_3)[x]$, which have no common zeroes in $\mathbb{C}$, of degrees $|\rho|^2$ and $|\rho|^2 - 1$, respectively, such that*

$$\wp(\rho z) = A_\rho(\wp(z))/B_\rho(\wp(z)). \tag{2.6}$$

Furthermore, if $p = (x, y)$, $\rho p \neq O$, and $\rho p \in E(F)$, then

$$[F(x, y) : F] \leqslant |\rho|^2.$$

Proof. See [2, Chap. 1].

LEMMA 2.3. *$E(F)$ is an $\mathcal{O}$-module with respect to addition on E and multiplication by elements of $\mathcal{O}$.*

Proof. It is easily seen from the addition theorem for $\wp(z)$ that $p_1 + p_2 \in E(F)$ for any $p_1, p_2 \in E(F)$. It remains to show that $\tau p \in E(F)$ for any $p \in E(F)$. We may suppose that $\tau p \neq O$, thus $p = (\wp(u), \wp'(u))$ for some $u \in \mathbb{C} \backslash \mathcal{L}$. From Lemma 2.2 we see that $\wp(\tau u) \in F$. By differentiating (2.6) with $\rho = \tau$ and putting $z = u$, we get $\wp'(\tau u) \in F$. Thus $\tau p = (\wp(\tau u), \wp'(\tau u)) \in E(F)$.

We now define the logarithmic absolute height $h(p)$ and the Néron–Tate height $\hat{h}(p)$ on $E(\bar{\mathbb{Q}})$. A thorough exposition can be found in Lang [16, Chap. IV]. For an algebraic point p on E (see (1.2)) given by $x = \alpha$, $y = \beta$, and a number field F containing α, define $H_F(p)$ by

$$H_F(p) = H_F(\alpha).$$

As before, the number

$$h(p) = \frac{1}{[F : \mathbb{Q}]} \log H_F(p)$$

is independent of F and is called the logarithmic absolute height of p. Define also $h(O) = 0$. It can be shown that for any point $p \in E(\bar{\mathbb{Q}})$ the limit

$$\hat{h}(p) = \lim_{m \to \infty} 2^{-2m} h(2^m p) \tag{2.7}$$

exists and satisfies

$$|h(p) - \hat{h}(p)| < \kappa \tag{2.8}$$

for some κ depending effectively on g_2, g_3. (For the effectiveness of κ see Zimmer [31].) We call $\hat{h}(p)$ the Néron–Tate height of p. It is known that $\hat{h}(p)$ is a quadratic form.

LEMMA 2.4 (Néron and Tate). *Let $p_1,\dots, p_n$ be any points of $E(\bar{\mathbb{Q}})$, and $m_1,\dots, m_n$ be any rational integers. Then*

$$\hat{h}(m_1 p_1 + \cdots + m_n p_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} \eta_{ij} m_i m_j$$

where

$$\eta_{ij} = \tfrac{1}{2}(\hat{h}(p_i + p_j) - \hat{h}(p_i) - \hat{h}(p_j)) \qquad (1 \leqslant i, j \leqslant n).$$

Proof. See [16, Chap. IV, Sects. 3, 4].

It follows from Lemma 2.4 that

$$\hat{h}(mp) = m^2 \hat{h}(p)$$

for any $m \in \mathbb{Z}$, $p \in E(\bar{\mathbb{Q}})$ and $\hat{h}$ vanishes exactly at the torsion points of E (i.e., the elements of finite order of the group E). Later we shall use the following

LEMMA 2.5. *For any p_1, p_2 in $E(\bar{\mathbb{Q}})$,*

$$(\hat{h}(p_1 + p_2))^{1/2} \leqslant (\hat{h}(p_1))^{1/2} + (\hat{h}(p_2))^{1/2}.$$

Proof. For any m_1, m_2 in $\mathbb{Z}$, by Lemma 2.4 we obtain

$$\hat{h}(m_1 p_1 + m_2 p_2) = a m_1^2 + 2b m_1 m_2 + c m_2^2, \tag{2.9}$$

where $a = \hat{h}(p_1)$, $b = \frac{1}{2}(\hat{h}(p_1 + p_2) - \hat{h}(p_1) - \hat{h}(p_2))$, $c = \hat{h}(p_2)$. If $a = c = 0$, then $p_1 + p_2$ is torsion whence $\hat{h}(p_1 + p_2) = 0$ and the lemma holds trivially. So we may assume that $a > 0$. Since $\hat{h} \geqslant 0$ on $E(\bar{\mathbb{Q}})$, the quadratic form $ax^2 + 2bxy + cy^2$ is non-negative on $\mathbb{Z}^2$, whence on $\mathbb{Q}^2$. Thus, by continuity, it is non-negative on $\mathbb{R}^2$. Therefore

$$b^2 \leqslant ac.$$

Put $m_1 = m_2 = 1$ in (2.9) to obtain

$$\hat{h}(p_1 + p_2) = a + 2b + c \leqslant (a^{1/2} + c^{1/2})^2.$$

This proves the lemma.

We now prove that for any $\rho \in \mathcal{O}$ and $p \in E(\bar{\mathbb{Q}})$,

$$\hat{h}(\rho p) = |\rho|^2 \hat{h}(p). \tag{2.10}$$

If $\rho = 0$, (2.10) is obvious. Suppose now that $\rho \neq 0$. By Lemma 2.2 and [16, Chap. IV, Theorem 1.1] we see that

$$h(2^m \rho p) - |\rho|^2 h(2^m p) = O(1),$$

where $O(1)$ is bounded on $E(\bar{\mathbb{Q}})$. This together with (2.7) implies (2.10). On combining Lemma 2.5 and (2.10) we obtain

LEMMA 2.6. *For any* $\rho_i \in \mathcal{O}$, $p_i \in E(\bar{\mathbb{Q}})$ $(1 \leqslant i \leqslant n)$,

$$\hat{h}(\rho_1 p_1 + \cdots + \rho_n p_n) \leqslant n(|\rho_1|^2 \hat{h}(p_1) + \cdots + |\rho_n|^2 \hat{h}(p_n)).$$

For an algebraic point p on E (see (1.2)) given by $x = \alpha$, $y = \beta$, we define the degree $d(p)$ of p as

$$d(p) = [k(g_2, g_3, \alpha, \beta): k(g_2, g_3)].$$

LEMMA 2.7 (Anderson and Masser [3]). *There is a constant* $\kappa_1 > 0$ *depending effectively on* g_2, g_3 *such that*

$$\hat{h}(p) \geqslant \kappa_1 D^{-3} (\log D)^{-2}$$

for any non-torsion $p \in E(\bar{\mathbb{Q}})$ *with* $d(p) \leqslant D$ $(D \geqslant 3)$.

Proof. See [3].

Remark. M. Laurent has shown in [17] that the lower bound in Lemma 2.7 can be improved by

$$\hat{h}(p) \geqslant \kappa_1' D^{-1} (\log D / \log \log D)^{-3}$$

for $D \geqslant e^e$ with the constant $\kappa_1' > 0$ depending effectively on g_2, g_3. This refinement is needed for the proof of our Theorem 2′. However, Lemma 2.7 is sufficient for the proof of Theorem 2.

For later references we quote a result from geometry of numbers. For $z \in \mathbb{C}$ denote by $\bar{z}$ its complex conjugate.

LEMMA 2.8. *Let* $r \geqslant 0$, $s \geqslant 1$ *be integers and* $n = r + 2s$. *Suppose that* $m_{ij} \in \mathbb{C}$ $(1 \leqslant i, j \leqslant n)$ *satisfy the following conditions*:

(1) $\det(m_{ij}) \neq 0$;

(2) $\bar{m}_{2i-1,j} = m_{2i,j}$ $(1 \leqslant i \leqslant s, 1 \leqslant j \leqslant n)$;

(3) m_{ij} $(2s + 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n)$ *are real numbers.*

Suppose further that $a_1, \ldots, a_n$ *are positive numbers such that* $a_{2i-1} = a_{2i}$ $(1 \leqslant i \leqslant s)$ *and*

$$\left(\frac{\pi}{2}\right)^s a_1 a_2 \cdots a_n \geqslant |\det(m_{ij})|.$$

Then there exist $x_1, \ldots, x_n$ *in* $\mathbb{Z}$, *not all zero, such that*

$$\left| \sum_{j=1}^{n} m_{ij} x_j \right| \leqslant a_i \qquad (i = 1, 2),$$

$$\left| \sum_{j=1}^{n} m_{ij} x_j \right| < a_i \qquad (3 \leqslant i \leqslant n).$$

(*Here the inequalities for* $3 \leqslant i \leqslant n$ *are absent if* $r = 0$, $s = 1$.)

Proof. See Weyl [27, pp. 162–163]. We remark that the product $b_1 \cdots b_{r_2}$ in [27, pp. 162–163] should be read as $(b_1 \cdots b_{r_2})^2$.

LEMMA 2.9. *There exists a constant* $\kappa_2 > 0$ *depending effectively on* g_2, g_3 *such that for any torsion point* p_0 *of* E *of order* $N \geqslant 2$

$$d(p_0) \geqslant \kappa_2 N / \log N.$$

Proof. We first prove the lemma for

$$N > (2/\pi)\,|\tau - \bar{\tau}|. \tag{2.11}$$

Recall $\tau = a\omega_2/\omega_1$ and put $N_1 = aN$. Obviously, we can write

$$p_0 = p\left(\frac{\alpha\omega_1}{aN}\right) = p\left(\frac{\alpha\omega_1}{N_1}\right) \tag{2.12}$$

for some $\alpha \in \mathcal{O}$, where $p(z) = (\wp(z), \wp'(z))$ for $z \notin \mathcal{L}$ as defined in Section 1. On applying Lemma 2.8 with $r = s = 1$, we see that there exist x_1, x_2, x_3 in $\mathbb{Z}$, not all zero, such that

$$|\alpha x_1 - N_1 x_2 - \tau N_1 x_3| \leqslant b N^{1/2}, \qquad |x_1| < N,$$

where $b = a((2/\pi)\,|\tau - \bar{\tau}|)^{1/2}$. Without loss of generality, we may suppose that $x_1 \geqslant 0$. Thus on writing $m = x_1$, $\rho = x_2 + x_3\tau$, we have

$$|m\alpha - \rho N_1| \leqslant b N^{1/2}, \tag{2.13}$$

$$0 \leqslant m < N. \tag{2.14}$$

Obviously $m \in \mathbb{Z}$, $\rho \in \mathcal{O}$, $(m, \rho) \neq (0, 0)$. We assert that $m \neq 0$. For otherwise we should have $\rho \neq 0$ and $|\rho N_1| \leqslant b N^{1/2}$ (by (2.13)), whence by $|\rho| = |\mathrm{Norm}(\rho)|^{1/2} \geqslant 1$ we should have $N \leqslant (2/\pi)\,|\tau - \bar{\tau}|$, a contradiction to (2.11). This and (2.14) give $0 < m < N$. Let

$$\sigma = m\alpha - \rho N_1. \tag{2.15}$$

Obviously $\sigma \in \mathscr{O}$. By $0 < m < N$ and (2.12), (2.15) we obtain

$$O \neq mp_0 = p\left(\frac{m\alpha\omega_1}{N_1}\right) = p\left(\frac{\sigma\omega_1}{N_1}\right) \tag{2.16}$$

since p_0 has order N.

Fix $F = k(g_2, g_3)$ and for $z_i \in \mathbb{C}\backslash\mathscr{L}$ $(1 \leqslant i \leqslant t)$ write $F(p(z_i): 1 \leqslant i \leqslant t)$ for the field $F(\wp(z_i), \wp'(z_i): 1 \leqslant i \leqslant t)$. Let F_{N_1} be the N_1-division field of $\wp(z)$, i.e.,

$$F_{N_1} = F(p(\omega_1/N_1), p(\omega_2/N_1)).$$

By Masser [20, Theorem], there exists a constant $c > 0$ depending effectively on g_2, g_3, such that

$$[F_{N_1} : F] > cN_1^2/\log N_1. \tag{2.17}$$

(Here the constant c should not be confused with that in our Theorem 1.) It follows from (2.16), (2.12), and Lemma 2.3 that

$$F\left(p\left(\frac{\sigma\omega_1}{N_1}\right)\right) = F(mp_0) \subseteq F(p_0) \subseteq F(p(\omega_1/N_1)). \tag{2.18}$$

So we have

$$[F_{N_1} : F] = [F_{N_1} : F(p(\omega_1/N_1))][F(p(\omega_1/N_1)) : F(p_0)][F(p_0) : F]. \tag{2.19}$$

Note that $\omega_2/N_1 = \tau\omega_1/(aN_1)$, so

$$F_{N_1} \subseteq F\left(p(\omega_1/N_1), p\left(\frac{\omega_1}{aN_1}\right)\right) = F\left(p\left(\frac{\omega_1}{aN_1}\right)\right),$$

whence by Lemma 2.2

$$[F_{N_1} : F(p(\omega_1/N_1))] \leqslant \left[F\left(p\left(\frac{\omega_1}{aN_1}\right)\right) : F(p(\omega_1/N_1))\right] \leqslant a^2. \tag{2.20}$$

Further, by (2.18), (2.16), (2.15), (2.13), and Lemma 2.2 we have

$$[F(p(\omega_1/N_1)) : F(p_0)] \leqslant \left[F(p(\omega_1/N_1)) : F\left(p\left(\frac{\sigma\omega_1}{N_1}\right)\right)\right] \leqslant |\sigma|^2 \leqslant b^2N. \tag{2.21}$$

On combining (2.17), (2.19)–(2.21) and recalling $N_1 = aN$, we see that there exists a constant $\kappa_2' > 0$ depending effectively on g_2, g_3 such that

$$d(p_0) = [F(p_0) : F] > cb^{-2}N/(\log N + \log a) \geqslant \kappa_2' N/\log N.$$

This proves the lemma for N satisfying (2.11). So Lemma 2.9 follows immediately.

Denote by $\sigma(z)$ the entire function with simple zeroes at the poles of $\wp(z)$. We have (see Whittaker and Watson [28, p. 447])

$$\sigma(z) = z \prod_{0 \neq \omega \in \mathscr{L}} \left(1 - \frac{z}{\omega}\right) \exp\left(\frac{z}{\omega} + \frac{z^2}{2\omega^2}\right).$$

LEMMA 2.10. *The functions $\sigma(z)$ and $(\sigma(z))^2 \wp(z)$ are entire and for $W \geqslant 1$ their maximum moduli on $|z| \leqslant W$ do not exceed $e^{c_3 W^2}$, where $c_3 > 0$ depends only on g_2, g_3.*

Proof. See Masser [19, p. 78].

LEMMA 2.11. *Suppose $w \in \mathbb{C}$ is not a pole of $\wp(z)$, such that $|w| \leqslant W$ and $|\wp(w)| \leqslant X$ for some $W \geqslant 1$ and $X \geqslant 1$. Then*

$$|\sigma(w)|^2 \geqslant X^{-1} e^{-c_4 W^2}$$

for some constant $c_4 > 0$ depending only on g_2, g_3.

Proof. See [3, p. 27].

LEMMA 2.12. *There exist constants c_5, c_6 depending on ω_1, ω_2 with $0 < c_5$, $c_6 < 1$ and $c_5 < \min_{0 \neq \omega \in \mathscr{L}} |\omega|$ such that for any $z \in \mathbb{C}$ with $0 < |z| < c_5$,*

$$|\wp(z)| > c_6 |z|^{-2}.$$

Proof. The assertion follows at once from the Laurent series of $\wp(z)$ at $z = 0$:

$$\wp(z) = z^{-2} + \sum_{n=1}^{\infty} (2n+1) s_{2n+2} z^{2n},$$

where

$$s_m = \sum_{0 \neq \omega \in \mathscr{L}} \frac{1}{\omega^m}.$$

(See, for instance, [16, p. 9].)

For any $R_i > 0$ $(1 \leqslant i \leqslant n)$, write

$$B(R_1, \ldots, R_n) = \{(z_1, \ldots, z_n) \in \mathbb{C}^n \mid |z_i| \leqslant R_i \ (1 \leqslant i \leqslant n)\}.$$

If $f(z_1,..., z_n)$ is continuous on $B(R_1,..., R_n)$ we write

$$|f|_{B(R_1,\ldots,R_n)} = \sup\{|f(z_1,..., z_n)| \mid (z_1,..., z_n) \in B(R_1,..., R_n)\}.$$

The essential tool of the analytic part of our proof of Theorem 1′ is the following

LEMMA 2.13 (Waldschmidt). *Suppose that* $T \geqslant 1$, $n \geqslant 1$ *are rational integers,* S, U, R_i, r_i $(1 \leqslant i \leqslant n)$ *are positive numbers, and* $\varphi_\lambda(z_1,..., z_n)$ $(1 \leqslant \lambda \leqslant T)$ *are continuous on and analytic in* $B(R_1,..., R_n)$. *Suppose further that*

$$3 \leqslant U, \qquad S \leqslant U; \tag{2.22}$$

$$e \leqslant \frac{R_1}{r_1} = \cdots = \frac{R_n}{r_n} \leqslant e^U; \tag{2.23}$$

$$\sum_{\lambda=1}^{T} |\varphi_\lambda|_{B(R_1,\ldots,R_n)} \leqslant e^U; \tag{2.24}$$

and

$$(8U)^{n+1} \leqslant TS\left(\log \frac{R_1}{r_1}\right)^n. \tag{2.25}$$

Then there exist rational integers $a_1,..., a_T$ *with*

$$0 < \max_{1 \leqslant \lambda \leqslant T} |a_\lambda| \leqslant e^S$$

such that the function

$$\Phi(z_1,..., z_n) = \sum_{\lambda=1}^{T} a_\lambda \varphi_\lambda(z_1,..., z_n)$$

satisfies

$$|\Phi|_{B(r_1,\ldots,r_n)} \leqslant e^{-U}.$$

Remark. Waldschmidt has shown that the lemma holds more generally in the case when (2.23) and (2.25) are replaced by

$$e \leqslant \frac{R_i}{r_i} \leqslant e^U \qquad (1 \leqslant i \leqslant n)$$

and

$$(8U)^{n+1} \leqslant TS \prod_{i=1}^{n} \log \frac{R_i}{r_i}$$

respectively. But we need only the lemma with conditions (2.23) and (2.25).

Proof of Lemma 2.13. Note that the case when $R_1 = \cdots = R_n$, $r_1 = \cdots = r_n$ is exactly Théorème 3.1 of [26]. Now write $R = R_1$, $r = r_1$, $b_i = r_i/r = R_i/R$. It is easily seen that the lemma follows at once on applying [26, Théorème 3.1] to the functions

$$\varphi_\lambda^0(z_1, \ldots, z_n) = \varphi_\lambda(b_1 z_1, \ldots, b_n z_n) \qquad (1 \leqslant \lambda \leqslant T).$$

Throughout this paper, by dependence of a constant on the elliptic curve E we mean that it may depend on g_2, g_3, ω_1, ω_2 and κ, κ_1, κ_2 occurring in (2.8), Lemma 2.7 and Lemma 2.9, respectively. In the sequel, let C and c_7, $c_8 \cdots$ denote positive constants depending effectively on n and E, except if otherwise indicated. The proof of Theorem 1′ is given in Sections 3–6 and Sections 9–14. In Sections 3, 4, and 6 we suppose that C is large enough to justify the subsequent estimates and keep the hypotheses of Theorem 1′. We will prove Theorems 2 and 2′ in Section 7 and deduce Theorem 1 from Theorem 1′ in Section 8.

3. Small Values

For any positive $q \in \mathbb{Z}$, we see from Lemma 2.9 that

$$d(p(2^{-q}\omega_1)) \geqslant \kappa_2 2^q/(q \log 2),$$

whence there is the least positive $q_0 \in \mathbb{Z}$ such that

$$p(2^{-q_0}\omega_1) \notin E(K).$$

This implies by Lemma 2.3 that

$$z_0 = 2^{-q_0}\omega_1 \notin \mathcal{O}u_0 + \cdots + \mathcal{O}u_n + \mathcal{L}. \tag{3.1}$$

Let K_1 denote the field generated by the numbers τ, g_2, g_3, $\wp(z_0)$, $\wp'(z_0)$, $\beta_1, \ldots, \beta_n$, $\wp(u_i)$, $\wp'(u_i)$ for $0 \leqslant i \leqslant n$, $u_i \notin \mathcal{L}$ over $\mathbb{Q}$, and put $N = [K_1 : \mathbb{Q}]$. Since $u_0, u_1, \ldots, u_n$ are linearly independent over k, there are at least n of them not in $\mathcal{L}$. It is easy to verify that

$$N \leqslant 4D, \tag{3.2}$$

for if $q_0 = 1$ this follows from (1.1) and the well-known fact that $\wp'(\omega_1/2) = 0$; if $q_0 \geqslant 2$ this follows from Lemma 2.2 and the fact that $O \neq p(2^{1-q_0}\omega_1) \in E(K)$.

Further it is well known that we can fix a basis of K_1 over $\mathbb{Q}$ of the form

$$\xi_v = \tau^{t_v} g_2^{q_v} g_3^{q_v'} \wp(z_0)^{l_v} \wp'(z_0)^{l_v'} \left(\prod_{i=1}^{n} \beta_i^{h_{iv}} \right) \cdot \prod_{\substack{j=0 \\ u_j \notin \mathscr{L}}}^{n} (\wp(u_j)^{m_{jv}} \wp'(u_j)^{m_{jv}'}) \qquad (1 \leqslant v \leqslant N), \tag{3.3}$$

where all the exponents $t_v, \ldots, m_{jv}'$ are non-negative rational integers not exceeding $N-1$. We now estimate $h(\xi_v)$. Note that for any algebraic α, α' satisfying

$$\alpha'^2 = 4\alpha^3 - g_2\alpha - g_3,$$

we have

$$h(\alpha') \leqslant c_7 \max(1, h(\alpha)) \tag{3.4}$$

by (2.2)–(2.4). Since $\hat{h}(p(z_0)) = 0$, we see that

$$h(\wp(z_0)) = |h(p(z_0)) - \hat{h}(p(z_0))| < \kappa$$

by (2.8). Thus $h(\wp'(z_0)) \leqslant c_7 \max(1, \kappa)$. Let c_8 be a constant satisfying

$$\begin{aligned} &c_8 \geqslant 1 + |\tau| \geqslant \log|\tau| = h(\tau), \\ &c_8 \geqslant \max(|\omega_1|, \kappa, h(\wp(z_0)), h(\wp'(z_0)), h(g_2), h(g_3)). \end{aligned} \tag{3.5}$$

From the definition of V_i and (3.4) we get

$$h(\wp(u_i)) \leqslant V_i, \qquad h(\wp'(u_i)) \leqslant c_7 V_i \tag{3.6}$$

for $0 \leqslant i \leqslant n$, $u_i \notin \mathscr{L}$. Now on combining (2.2), (2.3) and (3.2), (3.3), (3.5), (3.6) we obtain

$$\begin{aligned} h(\xi_v) &\leqslant 5c_8 N + nNW + N(1 + c_7)(V_0 + \cdots + V_n) \\ &\leqslant c_9 D(W + V_0 + \cdots + V_n), \qquad (1 \leqslant v \leqslant N), \end{aligned} \tag{3.7}$$

whence by (2.1), (3.2) we have

$$\log|\xi_v| \leqslant c_{10} D^2 (W + V_0 + \cdots + V_n) \qquad (1 \leqslant v \leqslant N). \tag{3.8}$$

Let

$$S_i^2 = C^s D^{n(n+1)} V_0 \cdots V_n V_i^{-1} (J + Z)^{n^2} Z^{-n(n+1)} \qquad (0 \leqslant i \leqslant n), \tag{3.9}$$

where $s = n^2 + n + 2$;

$$r_i = 2c_8 S_i, \qquad R_i = 2c_8 e^{(Z+1)/2} S_i \qquad (1 \leqslant i \leqslant n); \tag{3.10}$$

$$L = C^l D^{n(n+2)} V_0 \cdots V_n (J+Z)^{n^2+n-1} Z^{-n(n+2)}, \tag{3.11}$$

where $l = n^2 + 2n + 2 + (2n)^{-1} = s + n + (2n)^{-1}$;

$$M = C^{n+1} D^n (J+Z)^n Z^{-n}; \tag{3.12}$$

$$U = C^{l+1} D^{(n+1)^2} V_0 \cdots V_n (J+Z)^{n(n+1)} Z^{-n(n+2)}; \tag{3.13}$$

$$S = (2N)^{-1} U. \tag{3.14}$$

Write

$$f_1(z) = \wp(z)(\sigma(z))^2, \qquad f_2(z) = \sigma(z). \tag{3.15}$$

PROPOSITION 3.1. *For any rational integers $\lambda_1, \ldots, \lambda_n$, μ, ν with*

$$0 \leqslant \lambda_i \leqslant L \ (1 \leqslant i \leqslant n), \qquad 0 \leqslant \mu \leqslant M, \ 1 \leqslant \nu \leqslant N \tag{3.16}$$

there exists a rational integer $a_{\lambda,\mu,\nu}$ $(\lambda = (\lambda_1, \ldots, \lambda_n))$ satisfying

$$0 < \max_{\lambda,\ \mu,\ \nu} |a_{\lambda,\mu,\nu}| \leqslant e^S, \tag{3.17}$$

where the maximum is taken for all $\lambda = (\lambda_1, \ldots, \lambda_n)$, μ, ν in (3.16), *such that the function*

$$\begin{aligned} \Phi(z_1, \ldots, z_n) &= \sum_{\lambda,\mu,\nu} a_{\lambda,\mu,\nu} \xi_\nu z_1^{\lambda_1} \cdots z_n^{\lambda_n} (\wp(z_0 + u_1 z_1 + \cdots + u_n z_n))^\mu \\ &\quad \times (\sigma(z_0 + u_1 z_1 + \cdots + u_n z_n))^{2[M]} \\ &= \sum_{\lambda,\mu,\nu} a_{\lambda,\mu,\nu} \xi_\nu z_1^{\lambda_1} \cdots z_n^{\lambda_n} (f_1(z_0 + u_1 z_1 + \cdots + u_n z_n))^\mu \\ &\quad \times (f_2(z_0 + u_1 z_1 + \cdots + u_n z_n))^{2([M]-\mu)}, \end{aligned} \tag{3.18}$$

where the sums range over (3.16), *satisfies*

$$|\Phi|_{B(r_1,\ldots,r_n)} \leqslant e^{-U}. \tag{3.19}$$

Proof. Let

$$\begin{aligned} \varphi_{\lambda,\mu,\nu}(z_1, \ldots, z_n) &= \xi_\nu z_1^{\lambda_1} \cdots z_n^{\lambda_n} (f_1(z_0 + u_1 z_1 + \cdots + u_n z_n))^\mu \\ &\quad \times (f_2(z_0 + u_1 z_1 + \cdots + u_n z_n))^{2([M]-\mu)} \end{aligned}$$

for every (λ, μ, ν) in (3.16). It is easily seen that every $\varphi_{\lambda,\mu,\nu}$ is entire. We

now apply Lemma 2.13 to the φ's. Here $T=(\lfloor L\rfloor+1)^n(\lfloor M\rfloor+1)N$. We proceed to verify all the conditions (2.22)–(2.25) of Lemma 2.13.

From (3.13) and (1.5) we see that

$$U\geqslant C^{l+1}D^{n(n+1)}(DV_0)\cdots(DV_n)Z^{-n}\geqslant C^{l+1}D^{n(n+1)}Z\geqslant 3Z.$$

So

$$e\leqslant\frac{R_1}{r_1}=\cdots=\frac{R_n}{r_n}=e^{(Z+1)/2}\leqslant e^Z\leqslant e^U.$$

On combining these with (3.14), we conclude that (2.22) and (2.23) are satisfied.

To verify (2.24) we note that

$$\log(|z_1^{\lambda_1}\cdots z_n^{\lambda_n}|_{B(R_1,\ldots,R_n)})\leqslant L\log(R_1\cdots R_n)\leqslant c_{11}L(Z+\log(S_1\cdots S_n))$$
$$(0\leqslant\lambda_i\leqslant L,\ 1\leqslant i\leqslant n);\quad(3.20)$$

further, from (1.5) we see that

$$|u_i|^2\leqslant DV_ie^{1-Z},$$

so

$$(R_i|u_i|)^2\leqslant(2c_8e^{(Z+1)/2}S_i)^2DV_ie^{1-Z}\leqslant c_{12}DS_i^2V_i\qquad(1\leqslant i\leqslant n),$$

whence

$$|z_0+u_1z_1+\cdots+u_nz_n|^2_{B(R_1,\ldots,R_n)}\leqslant(c_8+R_1|u_1|+\cdots+R_n|u_n|)^2$$
$$\leqslant c_{13}D(S_1^2V_1+\cdots+S_n^2V_n)$$

by the Cauchy–Schwarz inequality, and this gives, by Lemma 2.10, that

$$\log|f_1(z_0+u_1z_1+\cdots+u_nz_n)^\mu f_2(z_0+u_1z_1+\cdots+u_nz_n)^{2([M]-\mu)}|_{B(R_1,\ldots,R_n)}$$
$$\leqslant c_{14}DM(S_1^2V_1+\cdots+S_n^2V_n)\qquad(0\leqslant\mu\leqslant M).\quad(3.21)$$

Thus, on combining (3.8), (3.20), (3.21), (3.2) and noting $M\geqslant D$ by (3.12), $S_0^2V_0=\cdots=S_n^2V_n$ by (3.9), $S_i^2\geqslant C^sD^{n^2}\geqslant 1$ by (3.9) and (1.5), we get

$$\log\sum_{\lambda,\mu,\nu}|\varphi_{\lambda,\mu,\nu}|_{B(R_1,\ldots,R_n)}$$
$$\leqslant c_{10}D^2(W+V_0+\cdots+V_n)+c_{11}L(Z+\log(S_0\cdots S_n))$$
$$+c_{14}DM(S_0^2V_0+\cdots+S_n^2V_n)+n\log(L+1)+\log(M+1)+\log N$$
$$\leqslant c_{10}D^2W+c_{15}L(Z+\log(S_0\cdots S_n))+c_{16}DM(S_0^2V_0+\cdots+S_n^2V_n)$$
$$\leqslant c_{17}(D^2W+LZ+L\log(S_0^2\cdots S_n^2)+DMS_0^2V_0),\quad(3.22)$$

where the sum ranges over (3.16). Now (1.5), (3.11), (3.13) yield $D \leqslant L$ and

$$D^2 WU^{-1} \leqslant DLWU^{-1} \leqslant C^{-1} \tag{3.23}$$

since $W \leqslant J = W + \log(DV)$. From (3.9) and (3.11)–(3.13) we obtain

$$LZU^{-1} \leqslant DL(J+Z)\,U^{-1} = C^{-1} \tag{3.24}$$

$$DMS_0^2 V_0 U^{-1} = C^{s+n+1-(l+1)} = C^{-(2n)^{-1}} \tag{3.25}$$

and

$$\begin{aligned} U^{-1}DL \log(S_0^2 \cdots S_n^2) &\leqslant U^{-1}DL((n+1)s \log C + n(n+1)^2 \log D \\ &\quad + n(n+1)\log V + n^2(n+1)\log(J+Z)) \\ &\leqslant c_{18} U^{-1} DL(J+Z)\log C \\ &\leqslant c_{18} C^{-1} \log C \leqslant C^{-1/2}. \end{aligned} \tag{3.26}$$

Thus, summing up (3.22)–(3.26), we obtain

$$\log \sum_{\lambda,\mu,\nu} |\varphi_{\lambda,\mu,\nu}|_{B(R_1,\ldots,R_n)} \leqslant c_{17}(2C^{-1} + C^{-1/2} + C^{-(2n)^{-1}})U \leqslant U.$$

This shows that (2.24) is satisfied. It remains to verify (2.25). We see from (3.10) – (3.14) that

$$\begin{aligned} &TS(\log(R_1/r_1))^n (8U)^{-(n+1)} \\ &\quad \geqslant L^n MN(2N)^{-1} U(Z/2)^n (8U)^{-(n+1)} \\ &\quad \geqslant 2^{-4(n+1)} L^n M Z^n U^{-n} \\ &\quad = 2^{-4(n+1)} C^{nl+n+1-n(l+1)} = 2^{-4(n+1)} C > 1. \end{aligned}$$

Thus (2.25), and therefore all the conditions of Lemma 2.13 are fulfilled. Now the conclusion of Proposition 3.1 follows from Lemma 2.13 immediately.

4. Many Zeroes

For later reference we first prove the following

Lemma 4.1. *If $f(z)$ is an entire function then for any $w_1, w_2 \in \mathbb{C}$ with $|w_1 - w_2| \leqslant 1$,*

$$|f(w_1) - f(w_2)| \leqslant 2\,|w_1 - w_2| \max_{|z| \leqslant w} |f(z)|,$$

where $w = 1 + \max(|w_1|, |w_2|)$.

Proof. Obviously, we may suppose that $w_1 \neq w_2$. Let $g(z) = (f(z) - f(w_2))/(z - w_2)$ if $z \neq w_2$ and $g(w_2) = f'(w_2)$; then $g(z)$ is an entire function. On applying the maximum-modulus theorem to $g(z)$ and the region $|z| \leqslant w$, we get

$$\left|\frac{f(w_1)-f(w_2)}{w_1-w_2}\right| = |g(w_1)| \leqslant \max_{|z|=w} |g(z)|$$

$$= \max_{|z|=w} \left|\frac{f(z)-f(w_2)}{z-w_2}\right| \leqslant 2 \max_{|z|=w} |f(z)|.$$

This proves the lemma.

In this section, we assume that the parameters S_i, r_i, R_i, L, M, U, S have been chosen in (3.9)–(3.14). For $\lambda = (\lambda_1, \ldots, \lambda_n)$, μ, ν in (3.16), let $a_{\lambda,\mu,\nu}$ be the rational integer in Proposition 3.1. Put

$$a_{\lambda,\mu} = \sum_{\nu=1}^{N} a_{\lambda,\mu,\nu}\xi_\nu$$

and

$$P(x_1, \ldots, x_n, y) = \sum_{\substack{0 \leqslant \lambda_i \leqslant L \\ 1 \leqslant i \leqslant n}} \sum_{0 \leqslant \mu \leqslant M} a_{\lambda_1,\ldots,\lambda_n,\mu} x_1^{\lambda_1} \cdots x_n^{\lambda_n} y^{\mu}. \tag{4.1}$$

Note that $P \neq 0$, since $\xi_1, \ldots, \xi_N$ form a basis for K_1 over $\mathbb{Q}$ and $a_{\lambda,\mu,\nu}$ are not all zero. For any $R > 0$ write $\mathscr{O}(R)$ for the set of elements ρ of $\mathscr{O}$ with

$$\rho = r + r'\tau, \qquad r, r' \in \mathbb{Z}, \qquad 0 \leqslant r, r' \leqslant R.$$

Write

$$\boldsymbol{\rho} = (\rho_0, \rho_1, \ldots, \rho_n) \in \mathscr{O}^{n+1}, \qquad \mathbf{u} = (u_0, u_1, \ldots, u_n),$$

$$\boldsymbol{\rho} \cdot \mathbf{u} = \rho_0 u_0 + \cdots + \rho_n u_n$$

and let $\mathscr{O}^{n+1}(S_0, \ldots, S_n)$ denote the set of $\boldsymbol{\rho} = (\rho_0, \ldots, \rho_n)$ with $\rho_i \in \mathscr{O}(S_i)$ $(0 \leqslant i \leqslant n)$. Recall that

$$\Lambda = \beta_1 u_1 + \cdots + \beta_n u_n - u_0$$

is the linear form in Theorem 1′.

PROPOSITION 4.1. *Suppose that*

$$|\Lambda| \leqslant e^{-3U}. \tag{4.2}$$

Then we have

$$P(\rho_1 + \rho_0\beta_1,\ldots,\rho_n + \rho_0\beta_n, \wp(z_0 + \boldsymbol{\rho}\cdot\mathbf{u})) = 0 \qquad \text{for all } \boldsymbol{\rho} \in \mathscr{O}^{n+1}(S_0,\ldots,S_n). \tag{4.3}$$

Proof. For an arbitrarily chosen $\boldsymbol{\rho} \in \mathscr{O}^{n+1}(S_0,\ldots,S_n)$ put

$$\Psi(\boldsymbol{\rho}) = P(\rho_1 + \rho_0\beta_1,\ldots,\rho_n + \rho_0\beta_n, \wp(z_0 + \boldsymbol{\rho}\cdot\mathbf{u}))(\sigma(z_0 + \boldsymbol{\rho}\cdot\mathbf{u}))^{2[M]}. \tag{4.4}$$

We first show that

$$|\Psi(\boldsymbol{\rho})| \leqslant 2e^{-U}. \tag{4.5}$$

Recall $\Lambda = \beta_1 u_1 + \cdots + \beta_n u_n - u_0$ and let

$$\begin{aligned} w_1 &= z_0 + \boldsymbol{\rho}\cdot\mathbf{u}, \\ w_2 &= z_0 + u_1(\rho_1 + \rho_0\beta_1) + \cdots + u_n(\rho_n + \rho_0\beta_n) = w_1 + \rho_0\Lambda, \\ f(z;\mu) &= (f_1(z))^{\mu}(f_2(z))^{2([M]-\mu)}, \end{aligned}$$

where f_1, f_2 are the functions defined in (3.15). On combining (3.18), (4.1), and (4.4), we obtain

$$\begin{aligned} &\Psi(\boldsymbol{\rho}) - \Phi(\rho_1 + \rho_0\beta_1,\ldots,\rho_n + \rho_0\beta_n) \\ &\quad = \sum_{\lambda,\mu,\nu}{}' a_{\lambda,\mu,\nu}\xi_\nu(\rho_1 + \rho_0\beta_1)^{\lambda_1}\cdots(\rho_n + \rho_0\beta_n)^{\lambda_n}(f(w_1;\mu) - f(w_2;\mu)), \end{aligned} \tag{4.6}$$

where the sum is taken over all λ, μ, ν in (3.16). Now

$$|w_1 - w_2| = |\rho_0|\,|\Lambda| \leqslant (1 + |\tau|)\,S_0 e^{-3U} \leqslant e^{-2U} < 1, \tag{4.7}$$

since $S_0^2 \leqslant C^{-2}U$ by (3.9) and (3.13). From (3.5), (4.7), and the inequality $V_i \geqslant \max(1, |u_i|^2/D)$ (by the definition of V_i) we get

$$\begin{aligned} w^2 = (1 + \max(|w_1|, |w_2|))^2 &\leqslant \left(|z_0| + \sum_{i=0}^{n} |\rho_i|\,|u_i| + 2\right)^2 \\ &\leqslant \left(c_8 + c_8 \sum_{i=0}^{n} S_i(DV_i)^{1/2} + 2\right)^2 \\ &\leqslant c_{19} D \sum_{i=0}^{n} S_i^2 V_i. \end{aligned} \tag{4.8}$$

So by Lemma 2.10 we have

$$\log \max_{|z| \leqslant w} |f(z;\mu)| \leqslant c_{20} DM \sum_{i=0}^{n} S_i^2 V_i \qquad (0 \leqslant \mu \leqslant M). \tag{4.9}$$

On applying Lemma 4.1 to $f(z;\mu)$, noting (4.7) and (4.9), we obtain

$$\log |f(w_1;\mu) - f(w_2;\mu)| \leqslant -2U + c_{21} DM \sum_{i=0}^{n} S_i^2 V_i \quad (0 \leqslant \mu \leqslant M). \tag{4.10}$$

Further, we see from (1.6), (3.5), (3.9) that

$$\begin{aligned} |\rho_i + \rho_0 \beta_i| &\leqslant c_8 (S_i + S_0 |\beta_i|) \\ &\leqslant c_8 (S_i + S_0 (V_0/V_i)^{1/2}) \\ &= 2c_8 S_i = r_i < R_i \qquad (1 \leqslant i \leqslant n). \end{aligned} \tag{4.11}$$

So, by (3.20)

$$\begin{aligned} &\log \max(1, |(\rho_1 + \rho_0 \beta_1)^{\lambda_1} \cdots (\rho_n + \rho_0 \beta_n)^{\lambda_n}|) \\ &\quad \leqslant c_{11} L(Z + \log(S_1 \cdots S_n)) \qquad (0 \leqslant \lambda_i \leqslant L,\ 1 \leqslant i \leqslant n). \end{aligned} \tag{4.12}$$

On combining (4.6), (3.17), (3.8), (4.12), (4.10), then combining (3.14), (3.12), (3.9), (3.2), and (3.23)–(3.26) we get

$$\begin{aligned} &\log |\Psi(\boldsymbol{\rho}) - \Phi(\rho_1 + \rho_0 \beta_1, \ldots, \rho_n + \rho_0 \beta_n)| \\ &\quad \leqslant S + c_{10} D^2 (W + V_0 + \cdots + V_n) + c_{11} L(Z + \log(S_1 \cdots S_n)) \\ &\qquad - 2U + c_{21} DM(S_0^2 V_0 + \cdots + S_n^2 V_n) \\ &\qquad + n \log(L+1) + \log(M+1) + \log N \\ &\quad \leqslant -(2 - (2N)^{-1}) U + c_{10} D^2 W \\ &\qquad + c_{22} L(Z + \log(S_0^2 \cdots S_n^2)) + c_{23} DMS_0^2 V_0 \\ &\quad \leqslant -U(2 - 1/2 - c_{10} C^{-1} - c_{22}(C^{-1} + C^{-1/2}) - c_{23} C^{-(2n)^{-1}}) \\ &\quad \leqslant -U. \end{aligned} \tag{4.13}$$

On the other hand Proposition 3.1 and (4.11) give

$$|\Phi(\rho_1 + \rho_0 \beta_1, \ldots, \rho_n + \rho_0 \beta_n)| \leqslant e^{-U}. \tag{4.14}$$

So (4.5) follows from (4.13) and (4.14) at once.

Next, by (2.8), Lemma 2.6, and the fact that $\hat{h}(p(z_0)) = 0$, $h(p_i) \leqslant V_i$ (by the definition of V_i), we get

$$\begin{aligned} h(\wp(z_0 + \boldsymbol{\rho} \cdot \mathbf{u})) &= h(p(z_0 + \boldsymbol{\rho} \cdot \mathbf{u})) \\ &\leqslant \hat{h}\Big(p(z_0) + \sum_{i=0}^{n} \rho_i p_i\Big) + \kappa \\ &\leqslant (n+2)\Big(\hat{h}(p(z_0)) + \sum_{i=0}^{n} |\rho_i|^2 \hat{h}(p_i)\Big) + \kappa \\ &\leqslant (n+2) \sum_{i=0}^{n} |\rho_i|^2 (V_i + \kappa) + \kappa \\ &\leqslant c_{24} \sum_{i=0}^{n} S_i^2 V_i. \end{aligned} \tag{4.15}$$

By Lemma 2.3, $\wp(z_0 + \boldsymbol{\rho} \cdot \mathbf{u})$ lies in K_1, so we see from (2.1), (4.15), and (3.2) that

$$\log |\wp(z_0 + \boldsymbol{\rho} \cdot \mathbf{u})| \leqslant c_{25} D \sum_{i=0}^{n} S_i^2 V_i. \tag{4.16}$$

Thus by Lemma 2.11, (4.16), (4.8), (3.9), and (3.25) we obtain

$$\begin{aligned} \log |\sigma(z_0 + \boldsymbol{\rho} \cdot \mathbf{u})|^{-2[M]} &\leqslant c_{26} DMS_0^2 V_0 \\ &= c_{26} C^{-(2n)^{-1}} U \leqslant C^{-(4n)^{-1}} U. \end{aligned} \tag{4.17}$$

On combining (4.4), (4.5), (4.17) we get

$$\begin{aligned} |P(\rho_1 + \rho_0\beta_1, \ldots, \rho_n + \rho_0\beta_n, \wp(z_0 + \boldsymbol{\rho} \cdot \mathbf{u}))| &\leqslant 2\exp(-(1 - C^{-(4n)^{-1}})U) \\ &\leqslant \exp(-(1 - C^{-(4n)^{-1}} - C^{-5})U), \end{aligned} \tag{4.18}$$

where the second inequality follows from the fact that $U \geqslant C^{l+1} > C^6 \geqslant C^5 \log 2$, a consequence of (3.13), (1.5), and $l = n^2 + 2n + 2 + (2n)^{-1}$ (see (3.11)).

Suppose

$$P(\rho_1 + \rho_0\beta_1, \ldots, \rho_n + \rho_0\beta_n, \wp(z_0 + \boldsymbol{\rho} \cdot \mathbf{u})) \neq 0. \tag{4.19}$$

We proceed to deduce a contradiction. Note that the left-hand side of (4.19) is in K_1 and is a polynomial Q in $\xi_1, \ldots, \xi_N$, $\rho_1 + \rho_0\beta_1, \ldots, \rho_n + \rho_0\beta_n$, $\wp(z_0 + \boldsymbol{\rho} \cdot \mathbf{u})$ with the coefficients $a_{\lambda,\mu,\nu} \in \mathbb{Z}$. By (3.17), its length satisfies

$$L(Q) \leqslant (L+1)^n (M+1) N e^S. \tag{4.20}$$

Further, by (2.2), (2.4),

$$h(\rho_i + \rho_0\beta_i) \leqslant h(\rho_i) + h(\rho_0) + h(\beta_i) + \log 2$$
$$\leqslant \log(c_8 S_i) + \log(c_8 S_0) + W + \log 2,$$

so

$$\sum_{i=1}^{n} h(\rho_i + \rho_0\beta_i) \leqslant c_{27}(W + \log(S_0 \cdots S_n)). \tag{4.21}$$

By (4.19) we can apply Lemma 2.1. On combining (4.20), (3.7), (4.21), (4.15), (3.14), (3.11), (3.9), (3.2), (3.23), (3.25), and (3.26) we obtain

$$\log |P(\rho_1 + \rho_0\beta_1, \ldots, \rho_n + \rho_0\beta_n, \wp(z_0 + \boldsymbol{\rho} \cdot \mathbf{u}))|$$
$$\geqslant -N(n \log(L+1) + \log(M+1) + \log N + S)$$
$$-N\Big(c_9 D(W + V_0 + \cdots + V_n)$$
$$+ C_{27} L(W + \log(S_0 \cdots S_n)) + c_{24} M \sum_{i=0}^{n} S_i^2 V_i\Big)$$
$$\geqslant -U/2 - c_{28} D(LW + L \log(S_0^2 \cdots S_n^2) + MS_0^2 V_0)$$
$$\geqslant -(\tfrac{1}{2} + c_{28}(C^{-1} + C^{-1/2} + C^{-(2n)^{-1}})). \tag{4.22}$$

Now it is easily seen that (4.22) contradicts (4.18) since C is large. This contradiction proves that (4.19) is impossible, i.e., $P(\rho_1 + \rho_0\beta_1, \ldots, \rho_n + \rho_0\beta_n, \wp(z_0 + \boldsymbol{\rho} \cdot \mathbf{u})) = 0$. Since $\boldsymbol{\rho} \in \mathscr{O}^{n+1}(S_0, \ldots, S_n)$ is arbitrarily chosen, the proof of Proposition 4.1 is complete.

5. The Proposition on Zero Estimate

Let $\wp(z)$ be the Weierstrass elliptic function in Theorem 1′. For $L > 0$, $M > 0$ let $L_0 = [L]$, $M_0 = [M]$. The algebraic part of the proof of Theorem 1′ consists of the proof of the following

Proposition 5.1. *Suppose that for $n \geqslant 1$, u_i $(0 \leqslant i \leqslant n)$, $\beta_j (1 \leqslant j \leqslant n)$, and z_0 are complex numbers such that*

$$u_0, \ldots, u_n \text{ are linearly independent over } k; \tag{5.1}$$
$$1, \beta_1, \ldots, \beta_n \text{ are linearly independent over } k; \tag{5.2}$$
$$z_0 \notin \mathscr{O}u_0 + \cdots + \mathscr{O}u_n + \mathscr{L}. \tag{5.3}$$

Let L, M, $S_0,\dots, S_n$ be positive numbers satisfying

$$nL_0 \geqslant 2^{n-1}M_0, \qquad M \geqslant \max(2, (2n)^n(n+2)^{-(n+2)}), \tag{5.4}$$

$$\min_{0\leqslant i_1<\cdots<i_{r+1}\leqslant n} S_{i_1}^2\cdots S_{i_{r+1}}^2 \geqslant c(r,n)\,L^r \qquad (1\leqslant r\leqslant n-1), \tag{5.5}$$

$$\min_{0\leqslant i_1<\cdots<i_n\leqslant n} S_{i_1}^2\cdots S_{i_n}^2 \geqslant C_1(n)\,L^{n-1}M, \tag{5.6}$$

$$S_0^2S_1^2\cdots S_n^2 \geqslant C_2(n)\,L^nM, \tag{5.7}$$

where

$$c(r,n) = 3\cdot 4^n n^r (n+1)^{2(r+1)},$$
$$C_1(n) = 3\cdot 4^{n-1}(n+1)^{3n+1},$$
$$C_2(n) = 3\cdot 2^n(n+1)^{2(n+1)}(n+2)^{n+2}.$$

(We assume that (5.5) is absent when $n=1$.) Suppose further that $P(x_1,\dots,x_n,y)\in\mathbb{C}[x_1,\dots,x_n,y]$ has degrees

$$\deg_{x_i} P \leqslant L (1\leqslant i\leqslant n), \qquad \deg_y P \leqslant M. \tag{5.8}$$

Then if

$$P(\rho_1+\rho_0\beta_1,\dots,\rho_n+\rho_0\beta_n, \wp(z_0+\boldsymbol{\rho}\cdot\mathbf{u})) = 0 \qquad \text{for all } \boldsymbol{\rho}\in\mathscr{O}^{n+1}(S_0,\dots,S_n) \tag{5.9}$$

we have

$$P(x_1,\dots,x_n,y) = 0.$$

We leave the proof of Proposition 5.1 to Sections 9–14. Now, we deduce Theorem 1′, assuming Proposition 5.1 is true.

6. Deduction of Theorem 1′ from Propositions 4.1 and 5.1

By the hypotheses of Theorem 1′, $u_0,\dots,u_n$ and $\beta_1,\dots,\beta_n$ in Theorem 1′ satisfy the conditions (5.1) and (5.2), respectively. Note also that z_0 defined by (3.1) satisfies (5.3). We now show that the parameters $S_0,\dots,S_n$, L, and M defined by (3.9), (3.11), (3.12) satisfy the conditions (5.4)–(5.7). We recall that C is large enough to justify the subsequent estimates (see the end of Section 2). We recall also the definitions of the parameters D and Z in Theorem 1′ (see (1.5)). So we have

$$D\geqslant 2, \qquad DV_i \geqslant Z \qquad (0\leqslant i\leqslant n). \tag{6.1}$$

It is easily seen that to verify (5.4) it suffices to show

$$L \geqslant 2^n M, \qquad M \geqslant 2^n.$$

Now from (3.11), (3.12), (6.1) we get

$$\begin{aligned} LM^{-1} &= C^{l-(n+1)} D^{n(n+1)} V_0 \cdots V_n (J+Z)^{n^2-1} Z^{-n(n+1)} \\ &\geqslant C^{l-(n+1)} D^{n(n+1)} V_0 \cdots V_n Z^{-(n+1)} \\ &\geqslant C^{n^2} D^{n^2-1} \geqslant C^{n^2} \geqslant 2^n \end{aligned}$$

and

$$M \geqslant C^{n+1} D^n \geqslant 2^n.$$

So (5.4) is satisfied. Next, by (3.9), (3.11), and (3.12) we obtain

$$S_0^2 \cdots S_n^2 (L^n M)^{-1} = C^{(n+1)s-nl-(n+1)} = C^{1/2} \geqslant C_2(n), \tag{6.2}$$

so (5.7) is fulfilled. Note now (3.9), (3.11), (6.1) imply

$$\begin{aligned} LS_i^{-2} &= C^{l-s} D^n V_i (J+Z)^{n-1} Z^{-n} \\ &\geqslant C^{l-s} D^n V_i Z^{-1} \geqslant C^{l-s} D^{n-1} \geqslant C^n \qquad (0 \leqslant i \leqslant n). \end{aligned} \tag{6.3}$$

It follows from (6.2) and (6.3) that if $n \geqslant 2$ then for r with $1 \leqslant r \leqslant n-1$

$$\begin{aligned} L^{-r} \min_{0 \leqslant i_1 < \cdots < i_{r+1} \leqslant n} S_{i_1}^2 \cdots S_{i_{r+1}}^2 &\geqslant S_0^2 \cdots S_n^2 (L^n M)^{-1} (L(\max_{0 \leqslant i \leqslant n} S_i)^{-2})^{n-r} \\ &\geqslant C^{1/2+n(n-r)} \geqslant C^n \geqslant c(r, n), \end{aligned}$$

so (5.5) is satisfied. Similarly

$$\begin{aligned} &(L^{n-1} M)^{-1} \min_{0 \leqslant i_1 < \cdots < i_n \leqslant n} S_{i_1}^2 \cdots S_{i_n}^2 \\ &\quad \geqslant S_0^2 \cdots S_n^2 (L^n M)^{-1} L(\max_{0 \leqslant i \leqslant n} S_i)^{-2} \geqslant C^n \geqslant C_1(n), \end{aligned}$$

thus (5.6) is fulfilled.

Recall that we have constructed by Proposition 3.1 a non-zero polynomial

$$0 \neq P(x_1, \ldots, x_n, y) \in \mathbb{C}[x_1, \ldots, x_n, y]$$

(see (4.1)), which satisfies (5.8) with L, M defined by (3.11), (3.12). Suppose that $|\Lambda| \leqslant e^{-3U}$ (U is defined by (3.13)), then Proposition 4.1 states that (5.9), with S_i ($0 \leqslant i \leqslant n$) defined by (3.9), is fulfilled by this polynomial P. We have thus shown that (5.1)–(5.9) hold. Hence Proposition 5.1 asserts

that we must have $P=0$, which contradicts the fact that $P\neq 0$. This contradiction proves that $|\Lambda| > e^{-3U}$, and therefore establishes Theorem 1′ with $c' = 3C^{l+1} = 3C^{n^2+2n+3+(2n)^{-1}}$.

7. Proofs of Theorems 2 and 2′

In this section we follow the notations introduced in Theorems 2 and 2′. As in Section 2, for $z\in\mathbb{C}$ denote by $\bar{z}$ its complex conjugate. We first derive the following Corollary of Lemma 2.8, then we prove Theorems 2 and 2′ in a way similar to the proof of Waldschmidt [25, Lemma 4.1].

Corollary of Lemma 2.8. *Suppose that $n\geqslant 2$, $a_1,\ldots,a_n$ are positive numbers satisfying*

$$a_1\cdots a_n \geqslant 2^n(\operatorname{Im}\tau/\pi)^{n/2}. \tag{7.1}$$

Then for any $(\alpha_1,\ldots,\alpha_{i-1},\alpha_{i+1},\ldots,\alpha_n)\in\mathbb{C}^{n-1}$ and integer i with $1\leqslant i\leqslant n$ there exists $\mathbf{0}\neq(\rho_1,\ldots,\rho_n)\in\mathscr{O}^n$ satisfying

$$|\rho_i|\leqslant a_i, \qquad |\rho_j-\rho_i\alpha_j| < a_j \qquad (1\leqslant j\leqslant n, j\neq i). \tag{7.2}$$

Proof. Without loss of generality, we may assume $i=1$. Write $\rho_l = x_l+\tau y_l$ with $x_l, y_l\in\mathbb{Z}$ $(1\leqslant l\leqslant n)$. (7.2) is equivalent to the set of inequalities

$$\begin{aligned} |x_1+\tau y_1| &\leqslant a_1,\\ |x_1+\bar{\tau}y_1| &\leqslant a_1,\\ |x_j+\tau y_j-\alpha_j x_1-\alpha_j\tau y_1| &< a_j\\ |x_j+\bar{\tau}y_j-\bar{\alpha}_j x_1-\bar{\alpha}_j\bar{\tau}y_1| &< a_j \end{aligned} \qquad (2\leqslant j\leqslant n). \tag{7.3}$$

The absolute value of the coefficients determinant of the above $2n$ linear forms in $x_1, y_1,\ldots,x_n,y_n$ is $|\bar{\tau}-\tau|^n = (2\operatorname{Im}\tau)^n$. Now (7.1) implies $(\pi/2)^n(a_1\cdots a_n)^2\geqslant(2\operatorname{Im}\tau)^n$. So we can apply Lemma 2.8 with $r=0$, $s=n$, to (7.3), and the conclusion of the Corollary follows immediately.

Proof of Theorem 2. Without loss of generality, we may assume that any $n-1$ elements from $u_1,\ldots,u_n$ are linearly independent over the field k. So $u_i\neq 0$ $(1\leqslant i\leqslant n)$ and there exists $\mathbf{0}\neq\boldsymbol{\rho}=(\rho_1,\ldots,\rho_n)\in\mathscr{O}^n$ such that

$$\rho_1u_1+\cdots+\rho_nu_n=0.$$

For any such $\boldsymbol{\rho}$ we have $\rho_i\neq 0$ $(1\leqslant i\leqslant n)$, according to the above

assumption. Fix $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$ to be one of such $\boldsymbol{\rho}$'s with $\max_{1 \leqslant i \leqslant n} |\sigma_i|$ minimal. So

$$\sigma_i \neq 0, \qquad \rho_1 \sigma_j = \sigma_1 \rho_j \qquad (1 \leqslant i, j \leqslant n).$$

Thus $|\sigma_1| \leqslant |\rho_1|$, since $\max_{1 \leqslant i \leqslant n} |\sigma_i|$ is minimal. Hence

$$|\sigma_i| \leqslant |\rho_i| \qquad (1 \leqslant i \leqslant n). \tag{7.4}$$

Let $d_0 = \min_{0 \neq \omega \in \mathscr{L}} |\omega|$. For an integer $m \geqslant 1$, denote by $\varphi^{-1}(m)$ the maximum of integers $l \geqslant 2$ such that there exists a torsion point p on the elliptic curve E of degree $d(p) \leqslant m$ and order l. Obviously $\varphi^{-1}(m)$ is well defined, since the point $p(\omega_1/2)$ is of order 2 and degree $d(p(\omega_1/2)) = 1$ by the well-known fact that $\wp'(\omega_1/2) = 0$ whence $\wp(\omega_1/2) \in k(g_2, g_3)$, and since the set of integers l in the definition of $\varphi^{-1}(m)$ is finite by Lemma 2.9. It is easily seen, by Lemma 2.9, that

$$\varphi^{-1}(D) \leqslant c_{29} D \log D \tag{7.5}$$

for some constant $c_{29} > 0$ depending effectively on κ_2, i.e., on g_2, g_3.

We now apply the Corollary of Lemma 2.8 with $i = 1$ to $a_1, \ldots, a_n$ and $\alpha_2, \ldots, \alpha_n$ with

$$a_j^{-1} = (n-1) \max((\kappa_1^{-1} \hat{h}(p_j) D^3 \log^2 D)^{1/2}, |u_j| \varphi^{-1}(D)/d_0) \qquad (2 \leqslant j \leqslant n), \tag{7.6}$$

$$\begin{aligned} &a_1 = 2^n (\operatorname{Im} \tau/\pi)^{n/2} (a_2 \cdots a_n)^{-1}, \\ &\alpha_j = \sigma_j/\sigma_1 \qquad (2 \leqslant j \leqslant n), \end{aligned} \tag{7.7}$$

and therefore see that there exists $\mathbf{0} \neq \boldsymbol{\delta} = (\delta_1, \ldots, \delta_n) \in \mathscr{O}^n$ satisfying

$$|\delta_1| \leqslant a_1, \qquad |\delta_j - \delta_1 \sigma_j/\sigma_1| < a_j \qquad (2 \leqslant j \leqslant n). \tag{7.8}$$

By the definition of $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$, $\sigma_1 u_1 + \cdots + \sigma_n u_n = 0$, so we have

$$\sum_{j=1}^{n} \delta_j u_j = \sum_{j=2}^{n} (\delta_j - \delta_1 \sigma_j/\sigma_1) u_j. \tag{7.9}$$

Denote by p_0 the point on the elliptic curve E corresponding to $\sum_{j=1}^{n} \delta_j u_j$. We now prove

$$\hat{h}(p_0) < \kappa_1 D^{-3} (\log D)^{-2}. \tag{7.10}$$

In fact, if $n = 2$ and p_2 is torsion, then p_0 is also torsion by (7.9), so $\hat{h}(p_0) = 0$ and (7.10) is obvious. So we may suppose that $n > 2$ or $n = 2$ with p_2 non-torsion. Then there exists p_j (with $2 \leqslant j \leqslant n$) non-torsion, i.e.,

$\hat{h}(p_j) > 0$, according to the assumption that $u_2, \ldots, u_n$ are linearly independent over k. Thus by Lemma 2.6 and (2.10), (7.9), (7.8), (7.6) we get

$$\begin{aligned}\hat{h}(p_0) &\leqslant (n-1) \sum_{j=2}^{n} |\delta_j - \delta_1 \sigma_j/\sigma_1|^2 \, \hat{h}(p_j) \\ &< (n-1) \sum_{j=2}^{n} a_j^2 \hat{h}(p_j) \\ &\leqslant \kappa_1 D^{-3} (\log D)^{-2},\end{aligned}$$

and (7.10) follows. Further, we show that p_0 is torsion. Suppose that p_0 is non-torsion. Then, by Lemma 2.3,

$$d(p_0) \leqslant [k(g_2, g_3, \wp(u_i), \wp'(u_i): 1 \leqslant i \leqslant n, u_i \notin \mathscr{L}): k(g_2, g_3)] \leqslant D. \quad (7.11)$$

Hence by Lemma 2.7, (7.11), and $D \geqslant 3$, we have

$$d(p_0) \geqslant \kappa_1 D^{-3} (\log D)^{-2},$$

a contradiction to (7.10). This contradiction shows that p_0 is torsion.

We now assert that there exists a positive integer l such that

$$l \leqslant \varphi^{-1}(D), \qquad l \sum_{j=1}^{n} \delta_j u_j \in \mathscr{L}. \quad (7.12)$$

For this is obvious if $p_0 = O$ (the point at infinity); if $p_0 \neq O$, then (7.11) holds, so (7.12) follows from (7.11) and the fact that p_0 is torsion of order $\geqslant 2$. From (7.9), (7.12), (7.8), (7.6) we see that

$$\begin{aligned}\left| l \sum_{j=1}^{n} \delta_j u_j \right| &= l \left| \sum_{j=2}^{n} (\delta_j - \delta_1 \sigma_j/\sigma_1) u_j \right| \\ &< \varphi^{-1}(D) \sum_{j=2}^{n} a_j |u_j| \\ &\leqslant d_0 = \min_{0 \neq \omega \in \mathscr{L}} |\omega|.\end{aligned}$$

This together with (7.12) shows that $l \sum_{j=1}^{n} \delta_j u_j = 0$, i.e., $\sum_{j=1}^{n} \delta_j u_j = 0$. Hence by (7.4) and (7.8) we have

$$|\sigma_1|^2 \leqslant |\delta_1|^2 \leqslant a_1^2. \quad (7.13)$$

It is easily seen from (7.5), (7.6), (2.8) that

$$a_j^{-2} \leqslant (n-1)^2 \max((\kappa+1)\kappa_1^{-1}, c_{29}^2 d_0^{-2}) V_j D^3 \log^2 D \qquad (2 \leqslant j \leqslant n).$$

This together with (7.7), (7.13) proves

$$|\sigma_1|^2 \leqslant (c_2(n-1)^2 D^3 \log^2 D)^{n-1} V_1 \cdots V_n / V_1$$

with

$$c_2 = (\max(1, 4 \operatorname{Im} \tau/\pi))^2 \max((\kappa+1)\kappa_1^{-1}, c_{29}^2 d_0^{-2}),$$

which depends effectively on the elliptic curve E. We can prove the same inequality for $|\sigma_i|^2$ with $i = 2,\ldots, n$ similarly, thereby completing the proof of Theorem 2.

Proof of Theorem 2′. The proof is almost the same as that of Theorem 2. One needs to replace (7.6) by

$$a_j^{-1} = (n-1)\max(\{(1/\kappa_1')\hat{h}(p_j) D(\log D/\log\log D)^3\}^{1/2}, |u_j|\varphi^{-1}(D)/d_0) \qquad (2 \leqslant j \leqslant n)$$

and replace (7.10) by

$$\hat{h}(p_0) < \kappa_1' D^{-1}(\log D/\log\log D)^{-3}.$$

Hence we conclude, by the result of Laurent [17] (see the remark below Lemma 2.7), that p_0 is torsion. Note also, by (2.8) and (2.5), that

$$\begin{aligned}\hat{h}(p_j) &< h(p_j) + \kappa = h(\wp(u_j)) + \kappa \\ &\leqslant \log A_j + \kappa \leqslant (\kappa+1)\log A_j.\end{aligned}$$

Further, by (7.5) and

$$|u_j| \leqslant \sup_{z \in \Pi} |z| \leqslant c_{30},$$

we have

$$|u_j|\varphi^{-1}(D)/d_0 \leqslant c_{29} c_{30} d_0^{-1} D \log D.$$

Thus

$$a_j^{-2} \leqslant (n-1)^2 \max((\kappa+1)/\kappa_1', (c_{29}c_{30}d_0^{-1})^2)(\log A_j) D^2 \log^2 D.$$

Now it is easy to write down the complete proof of Theorem 2′ with

$$c_2' = (\max(1, 4 \operatorname{Im} \tau/\pi))^2 \max((\kappa+1)/\kappa_1', (c_{29}c_{30}d_0^{-1})^2).$$

We omit the details here.

8. The Deductions of Theorem 1 and Its Corollary

We first deduce from Theorem 1′ the following

Corollary of Theorem 1′. *Under the hypotheses of Theorem* 1′, *letting* Y *satisfy* $1 \leqslant Y \leqslant \min_{0 \leqslant i \leqslant n} \log(eDV_i/|u_i|^2)$, *we have*

$$|\Lambda| = |\beta_1 u_1 + \cdots \beta_n u_n - u_0|$$
$$> \exp(-c_{31} D^{(n+1)^2} V_0 \cdots V_n (J+Y)^{n(n+1)} Y^{-n(n+2)})$$

for some constant $c_{31} > 0$.

Proof. Let

$$\lambda = \max(1 - 2\log c_5, 2 - \log c_6) > 2, \tag{8.1}$$

where c_5, c_6 (with $0 < c_5, c_6 < 1$ and $c_5 < \min_{0 \neq \omega \in \mathscr{L}} |\omega|$) are the constants in Lemma 2.12. We now prove

$$\log(eDV_i/|u_i|^2) \leqslant \lambda DV_i \qquad (0 \leqslant i \leqslant n). \tag{8.2}$$

This is equivalent to

$$e^{-\lambda DV_i} \cdot eDV_i \leqslant |u_i|^2 \qquad (0 \leqslant i \leqslant n). \tag{8.3}$$

From (8.1) and the inequality $ex \leqslant e^x$ for $x \geqslant 1$ we obtain

$$e^{-\lambda DV_i} \cdot eDV_i \leqslant e^{-(\lambda-1)DV_i} \leqslant \exp(DV_i \min(2\log c_5, \log c_6 - 1))$$
$$\leqslant \min(c_5^2, c_6 e^{-DV_i}) \qquad (0 \leqslant i \leqslant n), \tag{8.4}$$

since $c_5 < 1$, $c_6 < 1$. So (8.3) holds when $|u_i| \geqslant c_5$. When $|u_i| < c_5 < \min_{0 \neq \omega \in \mathscr{L}} |\omega|$, on noting $u_i \neq 0$ by hypotheses, we have $u_i \notin \mathscr{L}$. Then Lemma 2.12 implies that $\wp(u_i) \neq 0$ and

$$|u_i|^2 > c_6 |\wp(u_i)|^{-1} \geqslant c_6 e^{-DV_i}, \tag{8.5}$$

by (2.1) and the definition of V_i. Now (8.4) and (8.5) yield (8.3). So in both cases (8.3) holds, and therefore (8.2) is established.

By (8.2) we have

$$1 \leqslant Y \leqslant \min_{0 \leqslant i \leqslant n} \log(eDV_i/|u_i|^2) \leqslant \lambda \min_{0 \leqslant i \leqslant n} \min(DV_i, \log(eDV_i/|u_i|^2)).$$

Let $Z = \max(1, Y/\lambda)$. Then it is easily seen that Z satisfies (1.5) and

$$(J+Z)^{n(n+1)} Z^{-n(n+2)} \leqslant \lambda^{n(n+2)} (J+Y)^{n(n+1)} Y^{-n(n+2)}.$$

Hence by Theorem 1′, the Corollary holds with $c_{31} = c' \lambda^{n(n+2)}$.

Deduction of Theorem 1 *from the Corollary of Theorem* 1′

In this deduction we use notations of Theorem 1, so $n \geqslant 2$ throughout.

Case 1. $u_1,\ldots,u_n$ are linearly independent over k. Without loss of generality, we may assume that

$$|\beta_n|^2 V_n \geqslant |\beta_i|^2 V_i \qquad (1 \leqslant i \leqslant n-1).$$

Let $\beta_i' = -\beta_i/\beta_n$ $(1 \leqslant i \leqslant n-1)$. Then we have

$$V_n \geqslant |\beta_i'|^2 V_i \qquad (1 \leqslant i \leqslant n-1).$$

Write $|\beta_1 u_1 + \cdots \beta_n u_n| = |\Lambda| = |\beta_n|\,|\Lambda'|$, where

$$\Lambda' = \beta_1' u_1 + \cdots + \beta_{n-1}' u_{n-1} - u_n.$$

Obviously $\beta_1',\ldots,\beta_{n-1}'$ lie in the field K and they, together with 1, are linearly independent over k. Further, since $h(\beta_i') = h(-\beta_i/\beta_n) \leqslant h(\beta_i) + h(\beta_n)$ by (2.2) and (2.3), we have

$$W' = \max_{1 \leqslant i \leqslant n-1} h(\beta_i') \leqslant 2W, \tag{8.6}$$

$$J' = W' + \log(DV) \leqslant 2W + \log(DV). \tag{8.7}$$

On applying the Corollary of Theorem 1′ to Λ' and the field K, noting (8.6), (8.7), and

$$|\beta_n| \geqslant e^{-Dh(\beta_n)} \geqslant e^{-DW}$$

by Lemma 2.1, and noting

$$DW \leqslant \lambda^n D^{n^2} V_1 \cdots V_n (2W + \log(DV) + Y)^{n(n-1)} Y^{1-n^2}$$

by the fact that (8.2) is obviously true for u_i, D, V_i in Theorem 1 whence $Y(DV_i)^{-1} \leqslant \lambda$, we see that

$$\begin{aligned} |\Lambda| = |\beta_n|\,|\Lambda'| &> \exp(-DW - c_{32} D^{n^2} V_1 \cdots V_n (2W + \log(DV) + Y)^{n(n-1)} Y^{1-n^2}) \\ &\geqslant \exp(-c_{33} D^{n^2} V_1 \cdots V_n (W + \log(DV) + Y)^{n(n-1)} Y^{1-n^2}). \end{aligned}$$

So Theorem 1 is deduced in Case 1.

Case 2. $u_1,\ldots,u_n$ are linearly dependent over k. By the hypotheses of Theorem 1, $n \geqslant 2$ and $u_i \neq 0$ $(1 \leqslant i \leqslant n)$. So without loss of generality, we may suppose that for some r with $1 \leqslant r \leqslant n-1$, $u_1,\ldots,u_r$, are linearly independent over k, and $u_1,\ldots,u_r, u_i$ are linearly dependent over k for each i with $r+1 \leqslant i \leqslant n$. Note that $D = [K : \mathbb{Q}] \geqslant 4$, since there is some $\beta_j \notin k$ by the linear independence (over k) of $\beta_1,\ldots,\beta_n$. On applying Theorem 2 to

$u_1,\dots,u_r, u_i$ for each i with $r+1 \leqslant i \leqslant n$, we see that there exist some $\rho_{ij} \in \mathcal{O}$ $(1 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant r)$ such that

$$\rho_{i0} u_i = \sum_{j=1}^{r} \rho_{ij} u_j, \qquad \rho_{i0} \neq 0 \qquad (1 \leqslant i \leqslant n), \tag{8.8}$$

$$\rho_{i0} = \rho_{ii} = 1, \qquad \rho_{ij} = 0 \qquad (1 \leqslant i, j \leqslant r, j \neq i), \tag{8.9}$$

$$|\rho_{ij}|^2 \leqslant (c_2 n^2 D^3 \log^2 D)^r V^n \qquad (1 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant r). \tag{8.10}$$

It follows from (8.10) that

$$h(\rho_{ij}) \leqslant c_{34} \log(DV) \qquad (1 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant r). \tag{8.11}$$

By (8.8) we have

$$\begin{aligned} \Lambda &= \sum_{i=1}^{n} \beta_i \sum_{j=1}^{r} (\rho_{ij}/\rho_{i0})\, u_j \\ &= \sum_{j=1}^{r} \left(\sum_{i=1}^{n} \beta_i \rho_{ij}/\rho_{i0} \right) u_j = \sum_{j=1}^{r} \beta_j' u_j, \end{aligned}$$

where

$$\beta_j' = \sum_{i=1}^{n} \beta_i \rho_{ij}/\rho_{i0} \qquad (1 \leqslant j \leqslant r). \tag{8.12}$$

Note that $\beta_1',\dots,\beta_r'$ lie in K and the identity in $x_1,\dots,x_r$,

$$\sum_{j=1}^{r} \beta_j' x_j = \beta_1 x_1 + \cdots + \beta_r x_r + \sum_{i=r+1}^{n} \beta_i \sum_{j=1}^{r} (\rho_{ij}/\rho_{i0})\, x_j$$

(by (8.9), (8.12)), shows that $\beta_1',\dots,\beta_r'$ are linearly independent over k, since so are $\beta_1,\dots,\beta_n$ by the hypotheses of Theorem 1.

Thus if $r \geqslant 2$ we can apply the Case 1 to $\beta_1' u_1 + \cdots + \beta_r' u_r$ and the field K. Note that

$$V' = \max_{1 \leqslant j \leqslant r} V_j \leqslant V, \tag{8.13}$$

$$\begin{aligned} 1 \leqslant Y &\leqslant \min_{1 \leqslant i \leqslant n} \log(eDV_i/|u_i|^2) \\ &\leqslant \min_{1 \leqslant j \leqslant r} \log(eDV_j/|u_j|^2), \end{aligned} \tag{8.14}$$

$$\begin{aligned} W' = \max_{1 \leqslant j \leqslant r} h(\beta_j') &\leqslant \max_{1 \leqslant j \leqslant r} \left(\sum_{i=1}^{n} (h(\beta_i) + h(\rho_{ij}) + h(\rho_{i0})) + \log n \right) \\ &\leqslant c_{35}(W + \log(DV)) \end{aligned} \tag{8.15}$$

by (2.2)–(2.4) and (8.11), (8.12). On applying the Case 1, by (8.13)–(8.15) we get

$$|\Lambda| = \left| \sum_{i=1}^{n} \beta_i u_i \right| = |\beta_1' u_1 + \cdots + \beta_r' u_r|$$
$$> \exp(-c_{36} D^{r^2} V_1 \cdots V_r (W + \log(DV) + Y)^{r(r-1)} Y^{1-r^2}). \quad (8.16)$$

Let $J = W + \log(DV)$. Since (8.2) holds for u_i, D, V_i in Theorem 1, we have

$$1 \leqslant Y \leqslant \min_{1 \leqslant i \leqslant n} \log(eDV_i/|u_i|^2) \leqslant \lambda D \min_{1 \leqslant i \leqslant n} V_i. \quad (8.17)$$

Hence

$$\frac{(J+Y)^{r(r-1)} Y^{1-r^2}}{(J+Y)^{n(n-1)} Y^{1-n^2}} = (J+Y)^{n-r-(n^2-r^2)} Y^{n^2-r^2}$$
$$\leqslant Y^{n-r} \leqslant \lambda^{n-r} D^{n-r} V_{r+1} \cdots V_n, \quad (8.18)$$

since $n - r - (n^2 - r^2) < 0$ by $1 \leqslant r \leqslant n-1$. By (8.16) and (8.18) we obtain

$$|\Lambda| > \exp(-c_{37} D^{n^2} V_1 \cdots V_n (W + \log(DV) + Y)^{n(n-1)} Y^{1-n^2}),$$

so the Case 2 (with $r \geqslant 2$) of Theorem 1 is deduced.

It remains to verify the Case 2 with $r = 1$. Now $\Lambda = \sum_{i=1}^{n} \beta_i u_i = \beta_1' u_1$. By Lemma 2.1 and (8.15) we have

$$|\beta_1'| \geqslant e^{-Dh(\beta_1')} \geqslant \exp(-c_{35} D(W + \log(DV))) = e^{-c_{35} DJ}. \quad (8.19)$$

By (8.5), which is also valid for u_i, D, V_i in Theorem 1, we get

$$|u_1| \geqslant \min(c_5, (c_6 e^{-DV_1})^{1/2}) \geqslant e^{-c_{38} DV_1}. \quad (8.20)$$

Further by (8.17) we obtain

$$D^{n^2} V_1 \cdots V_n (J+Y)^{n(n-1)} Y^{1-n^2}$$
$$\geqslant D^{n^2} V_1 \cdots V_n \max(JY^{-n}, Y^{1-n})$$
$$\geqslant \lambda^{-n} \max(DJ, DV_1), \quad (8.21)$$

since $n \geqslant 2$ and $\lambda > 2$. Thus Theorem 1 for Case 2 with $r = 1$ follows from $\Lambda = \beta_1' u_1$ and (8.19)–(8.21) at once. Now the deduction of Theorem 1 is complete.

Deduction of the Corollary of Theorem 1 *from Theorem* 1

Let

$$R = \max(1, |u_1|^2, \ldots, |u_n|^2) \leqslant \max\left(1, \sup_{z \in \Pi} |z|^2\right) \leqslant c_{39}, \tag{8.22}$$

$$V_i = R \log A_i \ (1 \leqslant i \leqslant n), \qquad V = \max_{1 \leqslant i \leqslant n} V_i = R \log A_n, \tag{8.23}$$

$$W = \log B, \qquad Y = \log(D \log A_1). \tag{8.24}$$

Then $V_i \geqslant \log A_i \geqslant 1$, $V_i \geqslant R \geqslant |u_i|^2 \geqslant |u_i|^2/D$ $(1 \leqslant i \leqslant n)$. By (2.5) and $0 \neq u_i \in \Pi = \{t_1\omega_1 + t_2\omega_2 \mid 0 \leqslant t_1, t_2 < 1\}$ we have

$$h(p_i) = h(\wp(u_i)) \leqslant \log A_i \leqslant V_i \qquad (1 \leqslant i \leqslant n).$$

Thus

$$V_i \geqslant \max(1, h(p_i), |u_i|^2/D) \qquad (1 \leqslant i \leqslant n).$$

Similarly, by (2.5) we get

$$W = \log B \geqslant \max_{1 \leqslant i \leqslant n} h(\beta_i).$$

Now (8.22), (8.23), and the inequality $D \geqslant 4$ give

$$\begin{aligned} 1 \leqslant Y &= \log(D \log A_1) \leqslant \log(eD \log A_1) \\ &\leqslant \min_{1 \leqslant i \leqslant n} \log(eDR(\log A_i)/|u_i|^2) = \min_{1 \leqslant i \leqslant n} \log(eDV_i/|u_i|^2). \end{aligned}$$

By (8.22)–(8.24) we see that

$$\begin{aligned} &(W + \log(DV) + Y)^{n(n-1)} Y^{1-n^2} \\ &\quad \leqslant c_{40} \left(\frac{\log B + \log D + \log\log A_n}{\log D + \log\log A_1}\right)^{n(n-1)} (\log D + \log\log A_1)^{1-n} \\ &\quad \leqslant c_{40} \left(\frac{\log B + \log\log A_n}{\log\log A_1}\right)^{n(n-1)} (\log D + \log\log A_1)^{1-n} \\ &\quad \leqslant c_{40} (\log B + \log\log A_n)^{n(n-1)} (\log\log A_1)^{1-n^2}. \end{aligned} \tag{8.25}$$

Now, on applying Theorem 1, the Corollary follows from (8.22), (8.23), and (8.25) immediately.

9. The Group Variety, Translation Formulae, and Operators

To complete the proofs of Theorem 1′, Theorem 1, and its Corollary it remains only to prove Proposition 5.1. Sections 9–14 are devoted to the proof of Proposition 5.1. Throughout these sections, we keep the hypotheses of this Proposition.

In this paper we follow the point of view on group varieties of Hartshorne's book [13] (see also the paper of Masser and Wüstholz [22]). For $N \geqslant 1$, let $\mathbb{P}^N$ be the projective N-space over $\mathbb{C}$ and $\mathfrak{R}$ be its homogeneous coordinate ring. For any homogeneous ideal $\mathfrak{I}$ of $\mathfrak{R}$ we define its zero set to be $Z(\mathfrak{I}) = \{\alpha \in \mathbb{P}^N \mid f(\alpha) = 0$ for all homogeneous elements f of $\mathfrak{I}\}$. If Y is any subset of $\mathbb{P}^N$ we define its homogeneous ideal in $\mathfrak{R}$, denoted by $I(Y)$, to be the homogeneous ideal generated by

$$\{f \in \mathfrak{R} \mid f \text{ is homogeneous and } f(\alpha) = 0 \text{ for all } \alpha \in Y\}.$$

The topology on $\mathbb{P}^N$ is the Zariski topology. For any subset Y of $\mathbb{P}^N$ we write $\bar{Y}$ for its closure in $\mathbb{P}^N$. A quasi-projective variety G is an open subset of an irreducible projective variety V. Thus $\bar{G} = V$, and $\dim G = \dim V$ (see [13, p. 12]). When G is a group, its group laws correspond to morphisms from $G \times G$ to G and from G to G defining addition and inverse respectively (see [13, p. 23]). An algebraic subgroup H of G is a subgroup of G closed in G, and we have $\dim H = \dim \bar{H}$.

We now introduce the notations for Sections 9–14.

For $n \geqslant 1$, let $X_0, \ldots, X_n$ be the homogeneous variables associated with $\mathbb{P}^n$. Let G_a be the additive group of $\mathbb{C}$. The product G_a^n is isomorphic to a group variety $U_a = \mathbb{P}^n - Z(X_0)$, where $Z(X_0)$ is the hyperplane defined by $X_0 = 0$. For two points in U_a with homogeneous coordinates $(a_0, \ldots, a_n)$ and $(a_0', \ldots, a_n')$ respectively, their sum has homogeneous coordinates $b_0, \ldots, b_n$ with $b_0 = a_0 a_0'$ and

$$b_i = a_i a_0' + a_0 a_i' \qquad (1 \leqslant i \leqslant n).$$

Denote by E the elliptic curve in $\mathbb{P}^2$

$$Y_2^2 Y_0 - 4Y_1^3 + g_2 Y_0^2 Y_1 + g_3 Y_0^3 = 0, \tag{9.1}$$

where Y_0, Y_1, Y_2 are the homogeneous variables associated with $\mathbb{P}^2$. Since the polynomial on the left of (9.1) is irreducible in $\mathbb{C}[Y_0, Y_1, Y_2]$, E is an irreducible projective variety with $\dim E = 1$. Note that the functions

$$h_0(z) = (\sigma(z))^3, \qquad h_1(z) = \wp(z)\, h_0(z), \qquad h_2(z) = \wp'(z)\, h_0(z)$$

are entire and have no common zeroes. Thus for any $z \in \mathbb{C}$, the values

$h_0(z_0+z)$, $h_1(z_0+z)$, $h_2(z_0+z)$ are homogeneous coordinates of a point $\psi(z)$ in $\mathbb{P}^2$, and we obtain an analytic isomorphism ψ between the quotient $\mathbb{C}/\mathscr{L}$ and its image E in $\mathbb{P}^2$. After inheriting the usual law of addition on $\mathbb{C}$, $\psi(z_1)+\psi(z_2)=\psi(z_1+z_2)$, the elliptic curve E becomes a group variety, whose origin is $\psi(0)$.

Recall

$$\boldsymbol{\rho}\cdot\mathbf{u}=\rho_0u_0+\cdots+\rho_nu_n$$

for $\boldsymbol{\rho}=(\rho_0,\ldots,\rho_n)\in\mathscr{O}^{n+1}$ and $\mathbf{u}=(u_0,\ldots,u_n)$. Write

$$\mathscr{W}=\{\boldsymbol{\rho}\cdot\mathbf{u}\mid\boldsymbol{\rho}\in\mathscr{O}^{n+1}\}.$$

For later references we need a lemma which is a direct consequence of [22, Lemma 10].

LEMMA 9.1. *For every $\boldsymbol{\rho}\in\mathscr{O}^{n+1}$ there exist polynomials F_ρ, G_ρ, H_ρ in $\mathbb{C}[y_1, y_2]$ of total degrees at most 2 such that the function*

$$\phi_\rho(z)=H_\rho(\wp(z_0+z),\wp'(z_0+z))$$

is non-zero at every point of $\mathscr{W}$ and we have

$$\phi_\rho(z)\,\wp(z_0+z+\boldsymbol{\rho}\cdot\mathbf{u})=F_\rho(\wp(z_0+z),\wp'(z_0+z)),$$
$$\phi_\rho(z)\,\wp'(z_0+z+\boldsymbol{\rho}\cdot\mathbf{u})=G_\rho(\wp(z_0+z),\wp'(z_0+z)).$$

We now consider $G_a^n\times E$. Using the Segre Embedding φ (see [13, p. 13] and Hodge and Pedoe [14, pp. 93–100]), we may identify $\mathbb{P}^n\times\mathbb{P}^2$ with its image in $\mathbb{P}^N$, where $N=3n+2$. Let $\{Z_{ij}\mid i=0,\ldots,n;\ j=0,1,2\}$ be the homogeneous variables of $\mathbb{P}^N$ and

$$\mathfrak{R}=\mathbb{C}[\{Z_{ij}\}]. \tag{9.2}$$

The kernel $\mathfrak{S}$ of the homomorphism $\mathfrak{R}\to\mathbb{C}[X_0,\ldots,X_n,Y_0,Y_1,Y_2]$ which sends Z_{ij} to X_iY_j is the homogeneous ideal generated by the polynomials

$$Z_{ij}Z_{lm}-Z_{im}Z_{lj}\qquad 0\leqslant i,\ l\leqslant n,\ 0\leqslant j,\ m\leqslant 2. \tag{9.3}$$

Thus

$$\varphi(\mathbb{P}^n\times\mathbb{P}^2)=Z(\mathfrak{S}). \tag{9.4}$$

Write

$$G=\varphi(U_a\times E). \tag{9.5}$$

Obviously

$$\bar{G} = \varphi(\mathbb{P}^n \times E)$$

is an irreducible projective variety in $\mathbb{P}^N$ (see [13, p. 22]) and G is open in $\bar{G}$. Thus G is a quasi-projective variety. Let $\mathfrak{G} = I(G)$. Evidently

$$\mathfrak{G} = I(G) = I(\bar{G}) \supseteq (\mathfrak{S}, Z_{02}^2 Z_{00} - 4Z_{01}^3 + g_2 Z_{00}^2 Z_{01} + g_3 Z_{00}^3), \quad (9.6)$$

and $\mathfrak{G}$ is a homogeneous prime ideal of $\mathfrak{R}$. We identify $G_a^n \times E$ with G (we shall also write $G = G_a^n \times E$) and write simply $(a_1,..., a_n) \times \psi(z)$ for $\varphi((1, a_1,..., a_n) \times \psi(z))$, where $(1, a_1,..., a_n)$ denotes the point in $\mathbb{P}^n$ with homogeneous coordinates $1, a_1,..., a_n$. After defining the group law of G by

$$(a_1,..., a_n) \times \psi(z_1) + (b_1,..., b_n) \times \psi(z_2) = (a_1 + b_1,..., a_n + b_n) \times \psi(z_1 + z_2),$$

G becomes a group variety. We also define the multiplication by an element ρ of $\mathscr{O}$:

$$\rho \cdot ((a_1,..., a_n) \times \psi(z)) = (\rho a_1,..., \rho a_n) \times \psi(\rho z).$$

Denote by Γ the subgroup of G generated by the $2(n+1)$ elements

$$\begin{aligned} \gamma_0 &= (\beta_1,..., \beta_n) \times \psi(u_0), \\ \gamma_1 &= (1, 0,..., 0) \times \psi(u_1), \\ &\cdots \\ \gamma_n &= (0,..., 0, 1) \times \psi(u_n), \\ \gamma_i' &= \tau\gamma_i \qquad (0 \leqslant i \leqslant n). \end{aligned} \quad (9.7)$$

By (5.2) it is easily seen that Γ has rank $2(n+1)$ and that Γ is also an $\mathscr{O}$-module with a basis $\gamma_0,..., \gamma_n$ and rank (over $\mathscr{O}$) $n+1$. For $\boldsymbol{\rho} = (\rho_0,..., \rho_n) \in \mathscr{O}^{n+1}$ write

$$\gamma^{(\boldsymbol{\rho})} = \rho_0\gamma_0 + \cdots + \rho_n\gamma_n = (\rho_1 + \rho_0\beta_1,..., \rho_n + \rho_0\beta_n) \times \psi(\boldsymbol{\rho} \cdot \mathbf{u}). \quad (9.8)$$

Clearly, $\boldsymbol{\rho} \to \gamma^{(\boldsymbol{\rho})}$ is an $\mathscr{O}$-module isomorphism from $\mathscr{O}^{n+1}$ to Γ.

To write down the translation formulae we first introduce some maps between the rings

$$\mathfrak{R}, \qquad \mathfrak{R}_1 = \mathbb{C}[x_1,..., x_n, y_1, y_2], \qquad \mathfrak{R}_2 = \mathbb{C}[X_0,..., X_n, Y_0, Y_1, Y_2].$$

For any $0 \neq f \in \mathfrak{R}_1$ with d_1 as its total degree in $x_1,..., x_n$ and d_2 as its total degree in y_1, y_2, let $d = \max(d_1, d_2)$ and put

$$^{h_1}f = (X_0 Y_0)^d f\left(\frac{X_1}{X_0},..., \frac{X_n}{X_0}, \frac{Y_1}{Y_0}, \frac{Y_2}{Y_0}\right).$$

Set ${}^{h_1}0 = 0$. Thus ${}^{h_1}f \in \mathfrak{R}_2$ for any $f \in \mathfrak{R}_1$. We say that a monomial $Z_{i_1 j_1}^{t_1} \cdots Z_{i_m j_m}^{t_m} \in \mathfrak{R}$ $(t_i > 0,\ 1 \leqslant i \leqslant m)$ is a standard power-product if $i_1 \leqslant \cdots \leqslant i_m$ and $j_1 \leqslant \cdots \leqslant j_m$. Suppose that $P \in \mathfrak{R}_2$ is homogeneous of degree $d \geqslant 1$ in $X_0, \ldots, X_n$ and Y_0, Y_1, Y_2 respectively, then on writing $X_i Y_j = Z_{ij}$, we can express P as homogeneous polynomials of $\mathfrak{R}$ of degree d. Among those polynomials there exists an unique one being a linear combination of standard power-products (see [14, pp. 98–100]). We denote it by ${}^{s}P$. We also put ${}^{s}a = a$ for $a \in \mathbb{C}$. The composition

$$h = s \circ h_1 : f \to {}^{h}f$$

is a map from $\mathfrak{R}_1$ to the set of homogeneous polynomials in $\mathfrak{R}$.

Denote by $W^{(\rho)}$ the zero set of $Y_0^2 H_\rho(Y_1/Y_0, Y_2/Y_0)$ in $\mathbb{P}^2$, and write

$$U^{(\rho)} = \varphi(U_a \times (E - E \cap W^{(\rho)})).$$

Evidently $U^{(\rho)}$ is an open subset of G containing Γ. Now we write down our translation formulae as follows.

LEMMA 9.2. *For* $\boldsymbol{\rho} \in \mathscr{O}^{n+1}$, *let*

$$l_0 = 1, \qquad l_j = x_j + \rho_j + \rho_0 \beta_j \qquad (1 \leqslant j \leqslant n),$$

and $E_{i0}^{(\rho)}$, $E_{i1}^{(\rho)}$, $E_{i2}^{(\rho)}$ $(0 \leqslant i \leqslant n)$ *be the homogeneous polynomials of* $\mathfrak{R}$ *of degree* 2, *which differ from* ${}^{h}(l_i H_\rho(y_1, y_2))$, ${}^{h}(l_i F_\rho(y_1, y_2))$, ${}^{h}(l_i G_\rho(y_1, y_2))$ *only by some factors of shape* Z_{00}^{m} $(m \geqslant 0,\ m \in \mathbb{Z})$, *respectively. If* $g \in U^{(\rho)}$ *has homogeneous coordinates* $z_{00}, \ldots, z_{n2}$, *then* $g + \gamma^{(\rho)}$ *has homogeneous coordinates*

$$E_{ij}^{(\rho)}(z_{00}, \ldots, z_{n2}) \qquad (0 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant 2).$$

Proof. The lemma can be verified by virtue of Lemma 9.1 and direct calculations. We omit the details here.

We now define a system of homomorphisms $E(\boldsymbol{\rho})$ of $\mathfrak{R}$ for every $\boldsymbol{\rho} \in \mathscr{O}^{n+1}$. If $P(Z_{00}, \ldots, Z_{n2}) \in \mathfrak{R}$, we set

$$E(\boldsymbol{\rho})P = P(E_{00}^{(\rho)}, \ldots, E_{n2}^{(\rho)}).$$

If $P \neq 0$ is homogeneous of degree d than $E(\boldsymbol{\rho})P$ is homogeneous of degree $2d$. For a subset $\mathscr{S}$ of $\mathfrak{R}$ we define $E(\boldsymbol{\rho})\mathscr{S}$ as the set of all $E(\boldsymbol{\rho})P$ for P in $\mathscr{S}$.

Let $\mathscr{M}$ be the multiplicative set in $\mathfrak{R}$ consisting of all polynomials not vanishing at any point of Γ. Obviously $\mathscr{M} \neq \varnothing$ since $Z_{00} \in \mathscr{M}$ by (5.3). The following lemma is a direct consequence of [22, Lemma 2].

LEMMA 9.3. *For every* $\rho \in \mathscr{O}^{n+1}$ *we have*

$$E(\rho)\mathscr{M} \subseteq \mathscr{M}, \qquad E(\rho)\mathfrak{G} \subseteq \mathfrak{G}.$$

Similarly to [22, Sect. 3] we define translation operators acting on ideals of $\mathfrak{R}$. For an ideal $\mathfrak{I}$ of $\mathfrak{R}$ we denote by $\mathfrak{I}^*$ the contracted extension with respect to $\mathscr{M}$; this is the ideal of all $P \in \mathfrak{R}$ such that $QP \in \mathfrak{I}$ for some $Q \in \mathscr{M}$. For $\rho \in \mathscr{O}^{n+1}$ we write $(E(\rho)\mathfrak{I}, \mathfrak{G})$ for the ideal generated by the elements of $E(\rho)\mathfrak{I}$ together with those of $\mathfrak{G}$. We define the ideal $\mathscr{E}(\rho)\mathfrak{I}$ by

$$\mathscr{E}(\rho)\mathfrak{I} = (E(\rho)\mathfrak{I}, \mathfrak{G})^*.$$

If $\mathfrak{I}$ is a homogeneous ideal, so is $\mathscr{E}(\rho)\mathfrak{I}$.

We say that an ideal $\mathfrak{I}$ of $\mathfrak{R}$ is special if $\mathfrak{G} \subseteq \mathfrak{I}$ and $\mathfrak{I}^* = \mathfrak{I}$. If $\mathfrak{I}$ is special then every prime ideal of $\mathfrak{I}$ is special. Obviously $\mathfrak{G}$ is special. Put $\mathbf{0} = (0,..., 0) \in \mathscr{O}^{n+1}$.

LEMMA 9.4. *For any homogeneous ideal* $\mathfrak{I}$ of $\mathfrak{R}$ *and any* ρ, δ *in* $\mathscr{O}^{n+1}$ *we have* $\mathfrak{I} \subseteq \mathscr{E}(\mathbf{0})\mathfrak{I}$ *and* $\mathscr{E}(\rho+\delta)\mathfrak{I} = \mathscr{E}(\rho)\mathscr{E}(\delta)\mathfrak{I}$. *Furthermore if* $\mathfrak{I}$ *is special then* $\mathfrak{I} = \mathscr{E}(\mathbf{0})\mathfrak{I}$.

Proof. This is a direct consequence of [22, Lemma 3].

We recall that a non-zero proper ideal $\mathfrak{I}$ of $\mathfrak{R}$ has a well-defined rank r (in the sense of [10] and [21]) satisfying $1 \leqslant r \leqslant N+1$.

LEMMA 9.5. *Suppose* $\mathfrak{I}$ *is a non-zero proper special homogeneous ideal of* $\mathfrak{R}$ *and* $\rho \in \mathscr{O}^{n+1}$. *Then* $\mathscr{E}(\rho)\mathfrak{I}$ *is a non-zero proper special homogeneous ideal of the same rank as* $\mathfrak{I}$, *and if* $\mathfrak{I}$ *vanishes at the point* γ *of* Γ, *then* $\mathscr{E}(\rho)\mathfrak{I}$ *vanishes at* $\gamma - \gamma^{(\rho)}$. *Furthermore if* $\mathfrak{I}$ *is prime then* $\mathscr{E}(\rho)\mathfrak{I}$ *is prime.*

Proof. This is a direct consequence of [22, Lemma 4].

10. HOMOGENIZING AND DEHOMOGENIZING

We now define a map $a: \mathfrak{R} \to \mathfrak{R}_1 = \mathbb{C}[x_1,..., x_n, y_1, y_2]$. Set

$$^aZ_{00} = 1, \qquad ^aZ_{i0} = x_i \quad (i \neq 0), \qquad ^aZ_{0j} = y_j \quad (j \neq 0),$$

$$^aZ_{ij} = x_i y_j \quad (i \neq 0, j \neq 0), \qquad ^a(P(Z_{00},..., Z_{n2})) = P(^aZ_{00},..., ^aZ_{n2}) \quad (10.1)$$

for any $P(Z_{00},..., Z_{n2}) \in \mathfrak{R}$. Evidently, this map is a homomorphism from $\mathfrak{R}$ to $\mathfrak{R}_1$.

Let $U_{00} = \mathbb{P}^N - Z(Z_{00})$ and recall that $\mathfrak{S}$ is the homogeneous ideal of $\mathfrak{R}$ generated by (9.3). We assert that if $P \in \mathfrak{R}$ is homogeneous then

$$^aP = 0 \qquad \text{implies} \qquad P \in \mathfrak{S}, \qquad (10.2)$$

for ${}^aP = 0$ yields, by (10.1) and (9.4), that P vanishes on $Z(\mathfrak{S}) \cap U_{00}$ which is non-empty, and so is a quasi-projective variety, whence

$$P \in I(Z(\mathfrak{S}) \cap U_{00}) = I(Z(\mathfrak{S})) = \mathfrak{S}.$$

Recall the map h from $\mathfrak{R}_1$ to $\mathfrak{R}$ defined in Section 9. For any $f \in \mathfrak{R}_1$, $P \in \mathfrak{R}$, write

$${}^{ah}f = {}^a({}^hf), \qquad {}^{ha}P = {}^h({}^aP).$$

Obviously

$${}^{ah}f = f. \tag{10.3}$$

It follows from (10.2), (10.3) that given $f_1, f_2 \in \mathfrak{R}_1$ there is an integer $m \geqslant 0$ such that

$$Z_{00}^m \, {}^h(f_1 f_2) - {}^hf_1 \, {}^hf_2 \in \mathfrak{S}. \tag{10.4}$$

By (10.3) and Lemma 9.2 we see that for $0 \leqslant i \leqslant n$

$${}^aE_{i0}^{(\rho)} = l_i H_\rho, \qquad {}^aE_{i1}^{(\rho)} = l_i F_\rho, \qquad {}^aE_{i2}^{(\rho)} = l_i G_\rho,$$

where $l_0 = 1$, $l_i = x_i + \rho_i + \rho_0\beta_i$ $(1 \leqslant i \leqslant n)$, $H_\rho = H_\rho(y_1, y_2)$, $F_\rho = F_\rho(y_1, y_2)$, $G_\rho = G_\rho(y_1, y_2)$. Hence if $P \in \mathfrak{R}$ is homogeneous of degree $d \geqslant 0$ and ${}^aP = f(x_1, \ldots, x_n, y_1, y_2) \in \mathfrak{R}_1$ then

$$\begin{aligned}
{}^a(E(\boldsymbol{\rho})P) &= {}^a(P(E_{00}^{(\rho)}, \ldots, E_{n2}^{(\rho)})) \\
&= P({}^aE_{00}^{(\rho)}, \ldots, {}^aE_{n2}^{(\rho)}) \\
&= P(H_\rho, \ldots, (x_n + \rho_n + \rho_0\beta_n) G_\rho) \\
&= (H_\rho)^d P(1, \ldots, (x_n + \rho_n + \rho_0\beta_n) G_\rho / H_\rho) \\
&= (H_\rho)^d f(x_1 + \rho_1 + \rho_0\beta_1, \ldots, x_n + \rho_n + \rho_0\beta_n, F_\rho/H_\rho, G_\rho/H_\rho)
\end{aligned} \tag{10.5}$$

Next we assert that if $P \in \mathfrak{R}$ is homogeneous then three is an integer $m \geqslant 0$ such that

$$Z_{00}^m \, {}^{ha}P - P \in \mathfrak{S}. \tag{10.6}$$

To show this, we assume, as we may, that $P \neq 0$ and $P = Z_{00}^l P_1$, where Z_{00}^l is the highest power of Z_{00} that divides P. Then the total degrees with respect to $x_1, \ldots, x_n$ and to y_1, y_2 of ${}^aP = {}^aP_1$ do not exceed $\deg P_1$, whence ${}^{ha}P$ is homogeneous of degree at most $\deg P_1 = \deg P - l$. Let $m = \deg P - \deg {}^{ha}P$. We see that $m \geqslant 0$ and

$$Q = Z_{00}^m \, {}^{ha}P - P$$

is homogeneous and ${}^{a}Q = {}^{aha}P - {}^{a}P = 0$. Hence $Q \in \mathfrak{S}$ by (10.2), and (10.6) follows.

We now extend the maps h and a to ideals. We shall denote ideals in $\mathfrak{R}_1$ by small German letters and ideals in $\mathfrak{R}$ by capital German letters. Given an ideal $\mathfrak{a}$ in $\mathfrak{R}_1$, we define ${}^{h}\mathfrak{a}$ to be the homogeneous ideal in $\mathfrak{R}$ generated by $\{{}^{h}f | f \in \mathfrak{a}\}$ together with $\mathfrak{S}$. We define also a map from the set of all homogeneous ideals of $\mathfrak{R}$ containing $\mathfrak{S}$ to the set of all ideals of $\mathfrak{R}_1$. Let $\mathfrak{A}$ be such an ideal of $\mathfrak{R}$ and ${}^{a}\mathfrak{A}$ be the set of ${}^{a}P$ for all homogeneous polynomials $P \in \mathfrak{A}$. Then ${}^{a}\mathfrak{A}$ is an ideal of $\mathfrak{R}_1$, since if $f \in \mathfrak{R}_1$ and $0 \neq P_i \in \mathfrak{A}$ $(i = 1, 2)$ are homogeneous with $\deg P_1 - \deg P_2 = t \geqslant 0$, then $Q = {}^{h}f \cdot (P_1 - Z_{00}^{t} P_2) \in \mathfrak{A}$ is homogeneous, so

$$f({}^{a}P_1 - {}^{a}P_2) = {}^{a}Q \in {}^{a}\mathfrak{A}.$$

Note that the compositions ah and ha have the properties

$$ {}^{ah}\mathfrak{a} = \mathfrak{a}, \tag{10.7}$$

$$ {}^{ha}\mathfrak{A} \supseteq \mathfrak{A}, \tag{10.8}$$

$$ Z_{00}^{m}\, {}^{ha}\mathfrak{A} \subseteq \mathfrak{A} \qquad \text{for some integer } m \geqslant 0. \tag{10.9}$$

Equation (10.7) is obvious by (10.3) and ${}^{a}\mathfrak{S} = (0)$; (10.8) follows from the fact, which is implied by (10.6), that if P is any homogeneous polynomial in $\mathfrak{A}$ then P is also in ${}^{ha}\mathfrak{A}$. To see (10.9) we note, by definition, that ${}^{ha}\mathfrak{A}$ is generated by a set of ${}^{ha}P$ for finitely many homogeneous $P \in \mathfrak{A}$ together with $\mathfrak{S}$, since $\mathfrak{R}$ is noetherian. For each of these P, by (10.6) there is an integer $t = t(P) \geqslant 0$ such that $Z_{00}^{t}\, {}^{ha}P - P \in \mathfrak{S} \subseteq \mathfrak{A}$, so $Z_{00}^{t}\, {}^{ha}P \in \mathfrak{A}$. Thus (10.9) holds with m being the maximum of these $t(P)$.

By (10.8) and (10.9) we see that for any homogeneous prime ideal $\mathfrak{P}$ of $\mathfrak{R}$ with $Z_{00} \notin \mathfrak{P}$ and $\mathfrak{S} \subseteq \mathfrak{P}$ we have

$$ {}^{ha}\mathfrak{P} = \mathfrak{P}. \tag{10.10}$$

Henceforth every capital German letter (unless otherwise indicated) will denote a homogeneous ideal in $\mathfrak{R}$ containing $\mathfrak{S}$. For later references (see Sect. 14 below) we prove

LEMMA 10.1. *The mapping $a: \mathfrak{A} \to {}^{a}\mathfrak{A}$ maps the set of all homogeneous ideals of $\mathfrak{R}$ containing $\mathfrak{S}$ onto the set of all ideals in $\mathfrak{R}_1$. It has the following properties*:

(1) $\mathfrak{A} \supseteq \mathfrak{B} \Rightarrow {}^{a}\mathfrak{A} \supseteq {}^{a}\mathfrak{B}$.

(2) ${}^{a}(\mathfrak{A}\mathfrak{B}) = {}^{a}\mathfrak{A}\,{}^{a}\mathfrak{B}$.

(3) ${}^{a}(\mathfrak{A} \cap \mathfrak{B}) = {}^{a}\mathfrak{A} \cap {}^{a}\mathfrak{B}$.

(4) ${}^a(\sqrt{\mathfrak{A}}) = \sqrt{{}^a\mathfrak{A}}$.

(5) ${}^a\mathfrak{A} = \mathfrak{R}_1$ *if and only if* $\mathfrak{A}$ *contains* Z_{00}^m *for some integer* $m \geqslant 0$.

(6) ${}^a\mathfrak{A} = {}^a\mathfrak{B}$ *if and only if* $\mathfrak{A} : Z_{00}^s = \mathfrak{B} : Z_{00}^s$ *for some integer* $s \geqslant 0$ *(and hence also for all* s *sufficiently large).*

(7) *If* $\mathfrak{P} \supsetneqq \mathfrak{S}$ *is prime with* $\mathfrak{P} \not\ni Z_{00}$ *and has rank* s, *then* ${}^a\mathfrak{P}$ *is a non-zero proper prime ideal of rank* $r = s - 2n$.

(8) *If* $\mathfrak{Q} \supsetneqq \mathfrak{S}$ *is primary, which does not contain any power of* Z_{00}, *then* ${}^a\mathfrak{Q}$ *is a non-zero proper primary ideal, and if* $\mathfrak{P} = \sqrt{\mathfrak{Q}}$ *then* ${}^a\mathfrak{P} = \sqrt{{}^a\mathfrak{Q}}$.

(9) *If* $\mathfrak{A} = \bigcap_i \mathfrak{Q}_i$ *is an irredundant primary representation of* $\mathfrak{A}$, *all the* $\mathfrak{Q}_i$ *being homogeneous, then* ${}^a\mathfrak{A} = \bigcap_j {}^a\mathfrak{Q}_j$, *where the* $\mathfrak{Q}_j$ *are those primary components* $\mathfrak{Q}_i$ *of* $\mathfrak{A}$ *which do not contain any power of* Z_{00}, *and the representation* ${}^a\mathfrak{A} = \bigcap_j {}^a\mathfrak{Q}_j$ *is primary and irredundant.*

Proof. (1) is obvious, and (2) follows from the observation that $\mathfrak{A}$ and $\mathfrak{B}$ have finite homogeneous basis, say, $P_1, \ldots, P_l$ and $Q_1, \ldots, Q_m$, respectively, and then ${}^a\mathfrak{A}\,{}^a\mathfrak{B}$ has a basis $\{{}^a(P_iQ_j) \mid 1 \leqslant i \leqslant l,\ 1 \leqslant j \leqslant m\}$. The inclusion ${}^a(\mathfrak{A} \cap \mathfrak{B}) \subseteq {}^a\mathfrak{A} \cap {}^a\mathfrak{B}$ follows from (1). On the other hand if $f \in {}^a\mathfrak{A} \cap {}^a\mathfrak{B}$ then there are $0 \neq P_1 \in \mathfrak{A}$ and $0 \neq P_2 \in \mathfrak{B}$ such that P_1, P_2 are homogeneous and ${}^aP_1 = {}^aP_2 = f$. Without loss of generality, we may suppose that $t = \deg P_1 - \deg P_2 \geqslant 0$. Then $Q = P_1 - Z_{00}^t P_2$ is homogeneous and ${}^aQ = 0$, so by (10.2) $Q \in \mathfrak{S} \subseteq \mathfrak{B}$. Thus $P_1 = Q + Z_{00}^t P_2 \in \mathfrak{A} \cap \mathfrak{B}$ and $f = {}^aP_1 \in {}^a(\mathfrak{A} \cap \mathfrak{B})$. So ${}^a\mathfrak{A} \cap {}^a\mathfrak{B} \subseteq {}^a(\mathfrak{A} \cap \mathfrak{B})$. This proves (3).

If P is a homogeneous polynomial in $\sqrt{\mathfrak{A}}$, then $P^t \in \mathfrak{A}$ for some $t \geqslant 1$. So $({}^aP)^t = {}^a(P^t) \in {}^a\mathfrak{A}$, i.e., ${}^aP \in \sqrt{{}^a\mathfrak{A}}$. This shows that ${}^a(\sqrt{\mathfrak{A}}) \subseteq \sqrt{{}^a\mathfrak{A}}$. Conversely, if $f \in \sqrt{{}^a\mathfrak{A}}$ then $f^{t'} \in {}^a\mathfrak{A}$ for some $t' \geqslant 1$. Then $Z_{00}^m({}^hf)^{t'} \in \mathfrak{A}$ for some $m \geqslant 0$ by (10.4) and (10.9). So $Z_{00}^m\,{}^hf \in \sqrt{\mathfrak{A}}$ and $f = {}^a(Z_{00}^m\,{}^hf) \in {}^a(\sqrt{\mathfrak{A}})$. This proves $\sqrt{{}^a\mathfrak{A}} \subseteq {}^a(\sqrt{\mathfrak{A}})$. Hence (4) follows.

If $Z_{00}^m \in \mathfrak{A}$ then $1 = {}^a(Z_{00}^m) \in {}^a\mathfrak{A}$, so ${}^a\mathfrak{A} = \mathfrak{R}_1$. Conversely ${}^a\mathfrak{A} = \mathfrak{R}_1$ implies $1 \in {}^a\mathfrak{A}$, then (10.9) yields $Z_{00}^m = Z_{00}^m\,{}^h1 \in \mathfrak{A}$ for some $m \geqslant 0$. So (5) is established.

It is easily verified that

$$ {}^a(\mathfrak{A} : Z_{00}^s) = {}^a\mathfrak{A} \qquad (s = 0, 1, 2, \ldots). \tag{10.11} $$

Hence $\mathfrak{A} : Z_{00}^s = \mathfrak{B} : Z_{00}^s$ for some $s \geqslant 0$ imlies that ${}^a\mathfrak{A} = {}^a\mathfrak{B}$. On the other hand, since $\mathfrak{R}$ is noetherian there exists an integer $s \geqslant 0$ such that

$$ \mathfrak{A} : Z_{00}^s = \mathfrak{A} : Z_{00}^{s+1} = \cdots, \tag{10.12} $$

$$ \mathfrak{B} : Z_{00}^s = \mathfrak{B} : Z_{00}^{s+1} = \cdots. \tag{10.13} $$

We now assume ${}^a\mathfrak{A} = {}^a\mathfrak{B}$ and proceed to show that

$$ \mathfrak{A} : Z_{00}^s = \mathfrak{B} : Z_{00}^s. \tag{10.14} $$

By (10.11) and ${}^{a}\mathfrak{A} = {}^{a}\mathfrak{B}$ we obtain

$$ {}^{ha}(\mathfrak{A} : Z_{00}^{s}) = {}^{ha}(\mathfrak{B} : Z_{00}^{s}). \tag{10.15} $$

By (10.9) there exists $m \geqslant 0$ such that

$$ Z_{00}^{m}\ {}^{ha}(\mathfrak{A} : Z_{00}^{s}) \subseteq \mathfrak{A} : Z_{00}^{s}, $$

i.e.,

$$ {}^{ha}(\mathfrak{A} : Z_{00}^{s}) \subseteq \mathfrak{A} : Z_{00}^{s+m} = \mathfrak{A} : Z_{00}^{s} \tag{10.16} $$

by (10.12). On combining (10.8) and (10.16), we get $\mathfrak{A} : Z_{00}^{s} = {}^{ha}(\mathfrak{A} : Z_{00}^{s})$. Similarly we have $\mathfrak{B} : Z_{00}^{s} = {}^{ha}(\mathfrak{B} : Z_{00}^{s})$. Now (10.14) follows from (10.15) at once. Property (6) is thus established.

We now prove (7). By (10.2) and (5) we see that ${}^{a}\mathfrak{P}$ is non-zero proper. Suppose $f_1, f_2 \in \mathfrak{R}_1$ and $f_1 f_2 \in {}^{a}\mathfrak{P}$. Then by (10.4), (10.10), and $Z_{00} \notin \mathfrak{P}$, we have ${}^{h}f_1\ {}^{h}f_2 \in \mathfrak{P}$. Hence we get, say, ${}^{h}f_1 \in \mathfrak{P}$, so $f_1 = {}^{ah}f_1 \in {}^{a}\mathfrak{P}$. This proves that ${}^{a}\mathfrak{P}$ is prime. To show $r = s - 2n$, we remark that if $\mathfrak{p}$ is a non-zero proper prime ideal of $\mathfrak{R}_1$ then ${}^{h}\mathfrak{p}$ is a proper prime ideal containing $\mathfrak{S}$ strictly. For if $P_1 P_2 \in {}^{h}\mathfrak{p}$ with $P_1, P_2 \in \mathfrak{R}$ homogeneous then ${}^{a}P_1\ {}^{a}P_2 \in {}^{ah}\mathfrak{p} = \mathfrak{p}$ by (10.7), and we have, say, ${}^{a}P_1 \in \mathfrak{p}$, so ${}^{ha}P_1 \in {}^{h}\mathfrak{p}$, whence $P_1 \in {}^{h}\mathfrak{p}$. This proves that ${}^{h}\mathfrak{p}$ is prime. The facts that ${}^{h}\mathfrak{p} \neq \mathfrak{R}$ and ${}^{h}\mathfrak{p} \neq \mathfrak{S}$ follow from (10.7). Further note that there exist two chains of distinct prime ideals

$$ (0) \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_r = {}^{a}\mathfrak{P}, $$

$$ (0) \subset \mathfrak{P}_1 \subset \cdots \subset \mathfrak{P}_{2n} = \mathfrak{S}, $$

since rank ${}^{a}\mathfrak{P} = r$ and rank $\mathfrak{S} = 2n$ by $\mathfrak{S} = I(Z(\mathfrak{S})) = I(\varphi(\mathbb{P}^n \times \mathbb{P}^2))$ (see (9.4) and [13, pp. 6, 11]). According to the above remark and on applying (10.7), (10.10), we see that

$$ (0) \subset \mathfrak{P}_1 \subset \cdots \subset \mathfrak{P}_{2n} \subset {}^{h}\mathfrak{p}_1 \subset \cdots \subset {}^{h}\mathfrak{p}_r = {}^{ha}\mathfrak{P} = \mathfrak{P} $$

is a chain of distinct prime ideals. This proves $r + 2n \leqslant s$. On the other hand, since $\mathfrak{S}$ and $\mathfrak{P}$ have dimensions $N - 2n$ and $N - s$, respectively, there is a chain of distinct homogeneous prime ideals

$$ \mathfrak{S} = \mathfrak{P}_0' \subset \cdots \subset \mathfrak{P}_{s-2n}' = \mathfrak{P} $$

by virtue of Zariski and Samuel [30, Vol. II, p. 194, Corollary 4]. Hence we see, on noting ${}^{ha}\mathfrak{P}_i' = \mathfrak{P}_i'$ $(0 \leqslant i \leqslant s - 2n)$ by (10.10) and the fact that $Z_{00} \notin \mathfrak{P}$, that

$$ (0) \subset {}^{a}\mathfrak{P}_1' \subset \cdots \subset {}^{a}\mathfrak{P}_{s-2n}' = {}^{a}\mathfrak{P} $$

is a chain of distinct prime ideals. So $s-2n\leqslant r$. This together with $r+2n\leqslant s$ (shown above) proves $r=s-2n$. The proof of (7) is thus complete.

To show (8) it suffices to prove that ${}^a\mathfrak{Q}$ is primary, since the assertion that ${}^a\mathfrak{Q}$ is non-zero proper is obvious and ${}^a\mathfrak{P}=\sqrt{{}^a\mathfrak{Q}}$ follows from (4). Suppose that $f_1f_2\in{}^a\mathfrak{Q}$ with $f_1,f_2\in\mathfrak{R}_1$ and $f_1\notin{}^a\mathfrak{Q}$. Then by (10.4) and (10.9) we have $Z_{00}^m\,{}^hf_1\,{}^hf_2\in\mathfrak{Q}$ for some $m\geqslant 0$. Hence $Z_{00}^m\,{}^hf_2\in\sqrt{\mathfrak{Q}}=\mathfrak{P}$ since ${}^hf_1\notin\mathfrak{Q}$ by (10.3) and $f_1\notin{}^a\mathfrak{Q}$. We then have ${}^hf_2\in\mathfrak{P}$ since $Z_{00}^m\notin\mathfrak{P}$ by the fact that $\mathfrak{Q}$ does not contain any power of Z_{00}. Thus $f_2={}^{ah}f_2\in{}^a\mathfrak{P}$ by (10.3). This proves that ${}^a\mathfrak{Q}$ is primary. So (8) is established.

The first assertion of (9) follows by (3) and (5). The assertion that the representation ${}^a\mathfrak{A}=\bigcap_j{}^a\mathfrak{Q}_j$ is primary follows by (8). Note that ${}^a\mathfrak{P}_j$'s are distinct by (10.10) and $Z_{00}\notin\mathfrak{P}_j$. It remains to verify the irredundancy. Let ν be any one of the indices j, and let $\mathfrak{A}_\nu=\bigcap_{i\neq\nu}\mathfrak{Q}_i$. We have then $\mathfrak{A}_\nu\not\subseteq\mathfrak{Q}_\nu$ since $\bigcap_i\mathfrak{Q}_i$ is an irredundant representation. So $\mathfrak{A}_\nu:Z_{00}^s\not\subseteq\mathfrak{Q}_\nu$ for all $s\geqslant 0$. On the other hand, by $\mathfrak{A}\subseteq\mathfrak{Q}_\nu$ and the definition of ν, we have

$$\mathfrak{A}:Z_{00}^s\subseteq\mathfrak{Q}_\nu:Z_{00}^s=\mathfrak{Q}_\nu\qquad(s=0,1,2,\ldots).$$

So $\mathfrak{A}_\nu:Z_{00}^s\neq\mathfrak{A}:Z_{00}^s$ for all $s\geqslant 0$. This and (6) show that ${}^a\mathfrak{A}\neq{}^a\mathfrak{A}_\nu$, i.e., ${}^a\mathfrak{A}\neq\bigcap_{j\neq\nu}{}^a\mathfrak{Q}_j$. This proves the irredundancy. The proof of (9), and therefore of the Lemma, is complete.

We now introduce

DEFINITION 10.1. A homogeneous prime ideal $\mathfrak{P}$ of $\mathfrak{R}$ is called good if there exist $a_1,\ldots,a_n$ in $\mathbb{C}$ such that

$$x_i-a_i\in{}^a\mathfrak{P}\qquad(1\leqslant i\leqslant n).\tag{10.17}$$

Otherwise $\mathfrak{P}$ is called bad.

LEMMA 10.2. *Suppose that for $m\geqslant 1$, $\mathfrak{P}_1,\ldots,\mathfrak{P}_m$ are bad homogeneous prime ideals. Then there exists a linear form*

$$\zeta=a_1x_1+\cdots+a_nx_n\neq 0$$

with $a_i\in\mathbb{C}$ $(1\leqslant i\leqslant n)$ such that

$${}^a\mathfrak{P}_i\cap\mathbb{C}[\zeta]=(0)\qquad(1\leqslant i\leqslant m).$$

Proof. Write $V=\{\xi=b_1x_1+\cdots+b_nx_n\mid(b_1,\ldots,b_n)\in\mathbb{C}^n\}$ and ${}^a\mathfrak{P}_i=\mathfrak{p}_i$ $(1\leqslant i\leqslant m)$. Let

$$V_i=\{\xi\mid\xi\in V,\mathbb{C}[\xi]\cap\mathfrak{p}_i\neq(0)\}\cup\{0\}\qquad(1\leqslant i\leqslant m).$$

Then V_i is a subspace of the linear space V over $\mathbb{C}$, for if $\xi \in V_i$ and $b \in \mathbb{C}$ then $b\xi \in V_i$, and if $\xi_1, \xi_2 \in V_i$ with $\xi_1 \neq 0$, $\xi_2 \neq 0$ and $\xi_1 + \xi_2 \neq 0$, then there exist $\theta_j \in \mathbb{C}$ $(j = 1, 2)$ such that $\xi_j - \theta_j \in \mathfrak{p}_i$ $(j = 1, 2)$ (since $\mathfrak{p}_i$ is a proper prime ideal of $\mathfrak{R}_1$ by Lemma 10.1 and the hypothesis, and since $\mathfrak{p}_i$ contains elements of $\mathbb{C}[\xi_j]$ $(j = 1, 2)$ of degree $\geqslant 1$ by the facts that $\mathbb{C}[\xi_j] \cap \mathfrak{p}_i \neq (0)$ $(j = 1, 2)$ and $\mathfrak{p}_i \neq \mathfrak{R}_1$), so $\xi_1 + \xi_2 - (\theta_1 + \theta_2) \in \mathfrak{p}_i$, whence $\xi_1 + \xi_2 \in V_i$. Moreover, since $\mathfrak{P}_i$ is bad there exists a $j = j(i)$ with $1 \leqslant j \leqslant n$ such that $x_j - \theta \notin \mathfrak{p}_i$ for any $\theta \in \mathbb{C}$, so $x_j \notin V_i$ by the facts that $\mathfrak{p}_i$ is prime and $\mathfrak{p}_i \neq \mathfrak{R}_1$ again. Hence $V_i \neq V$ $(1 \leqslant i \leqslant m)$. So $V - \bigcup_{i=1}^{m} V_i \neq \varnothing$ and we can take ζ to be any linear form in $V - \bigcup_{i=1}^{m} V_i$. This completes the proof of Lemma 10.2.

We recall the definitions of the multiplicative set $\mathscr{M}$ and special ideals in $\mathfrak{R}$ introduced in Section 9. For any special homogeneous prime ideal $\mathfrak{P}$ we define the stabilizer $S(\mathfrak{P})$ to be

$$S(\mathfrak{P}) = \{\boldsymbol{\rho} \in \mathscr{O}^{n+1} \mid \mathscr{E}(\boldsymbol{\rho})\mathfrak{P} = \mathfrak{P}\}. \tag{10.18}$$

LEMMA 10.3. *Suppose that $\mathfrak{P}$ is a good proper special homogeneous prime ideal. Then*

(1) $Z_{i0} - a_i Z_{00} \in \mathfrak{P}$ *for some* $a_i \in \mathbb{C}$ $(1 \leqslant i \leqslant n)$.

(2) $S(\mathfrak{P}) = \{\mathbf{0}\}$.

(3) $\mathscr{E}(\boldsymbol{\rho})\mathfrak{P}$ *is a good proper special homogeneous prime ideal for every* $\boldsymbol{\rho} \in \mathscr{O}^{n+1}$.

Proof. By Definition 10.1, we have $x_i - a_i \in {}^{a}\mathfrak{P}$ for some $a_i \in \mathbb{C}$ $(1 \leqslant i \leqslant n)$. Note that $Z_{00} \notin \mathfrak{P}$ since $\mathfrak{P}$ is special and $Z_{00} \in \mathscr{M}$. So

$$Z_{i0} - a_i Z_{00} = {}^{h}(x_i - a_i) \in {}^{ha}\mathfrak{P} = \mathfrak{P} \qquad (1 \leqslant i \leqslant n)$$

by (10.10). This proves (1).

Suppose now $\boldsymbol{\rho} \in S(\mathfrak{P})$. Then $\mathscr{E}(\boldsymbol{\rho})\mathfrak{P} = \mathfrak{P}$. By Lemma 9.4 we see that

$$\mathscr{E}(-t\boldsymbol{\rho})\mathfrak{P} = \mathfrak{P} \qquad (t = 1, 2, \ldots).$$

This and (1) show that

$$Z_{i0} - a_i Z_{00} \in \mathscr{E}(-t\boldsymbol{\rho})\mathfrak{P} \qquad (1 \leqslant i \leqslant n,\ t = 1, 2, \ldots). \tag{10.19}$$

Since $\mathfrak{P}$ is a proper special homogeneous prime ideal, $\mathfrak{P}$ vanishes at some point of Γ, say,

$$\gamma^{(\boldsymbol{\sigma})} = (\sigma_1 + \sigma_0\beta_1, \ldots, \sigma_n + \sigma_0\beta_n) \times \psi(\boldsymbol{\sigma} \cdot \mathbf{u})$$

(see [22, p. 495]), where $\boldsymbol{\sigma} = (\sigma_0, ..., \sigma_n) \in \mathcal{O}^{n+1}$. Now (10.19) and Lemma 9.5 imply that

$$\sigma_i + \sigma_0\beta_i + t(\rho_i + \rho_0\beta_i) - a_i = 0 \qquad (1 \leqslant i \leqslant n, t = 1, 2, ...).$$

This together with (5.2) yields $\rho_0 = \cdots = \rho_n = 0$. So $\boldsymbol{\rho} = \mathbf{0}$, and (2) follows.

By Lemma 9.5, we see that $\mathscr{E}(\boldsymbol{\rho})\mathfrak{P}$ is a proper special homogeneous prime ideal for any $\boldsymbol{\rho} \in \mathcal{O}^{n+1}$. It remains to verify that $\mathscr{E}(\boldsymbol{\rho})\mathfrak{P}$ is good. We remark that

$$^hH_{\boldsymbol{\rho}} \notin \mathscr{E}(\boldsymbol{\rho})\mathfrak{P} \tag{10.20}$$

since $^hH_{\boldsymbol{\rho}} \in \mathscr{M}$ by Lemma 9.1. Further

$$^{ha}(\mathscr{E}(\boldsymbol{\rho})\mathfrak{P}) = \mathscr{E}(\boldsymbol{\rho})\mathfrak{P} \tag{10.21}$$

by (10.10) and $Z_{00} \notin \mathscr{E}(\boldsymbol{\rho})\mathfrak{P}$. Now (1) implies

$$E(\boldsymbol{\rho})(Z_{i0} - a_i Z_{00}) \in \mathscr{E}(\boldsymbol{\rho})\mathfrak{P} \qquad (1 \leqslant i \leqslant n).$$

So by (10.5) we have

$$H_{\boldsymbol{\rho}} \cdot (x_i + \rho_i + \rho_0\beta_i - a_i) \in {}^a(\mathscr{E}(\boldsymbol{\rho})\mathfrak{P}) \qquad (1 \leqslant i \leqslant n).$$

Thus

$$x_i + \rho_i + \rho_0\beta_i - a_i \in {}^a(\mathscr{E}(\boldsymbol{\rho})\mathfrak{P}) \qquad (1 \leqslant i \leqslant n),$$

since ${}^a(\mathscr{E}(\boldsymbol{\rho})\mathfrak{P})$ is prime by Lemma 10.1 (7) and since $H_{\boldsymbol{\rho}} \notin {}^a(\mathscr{E}(\boldsymbol{\rho})\mathfrak{P})$ by (10.20) and (10.21). Hence $\mathscr{E}(\boldsymbol{\rho})\mathfrak{P}$ is good. The proof of (3), and therefore of the lemma, is complete.

11. Calculation of $p_1, ..., p_{n+1}$

It can be shown that for $1 \leqslant r \leqslant n+1$ there is a connected algebraic subgroup of $G = G_a^n \times E$ (introduced in Section 9) of codimension r (see Lemma 11.1 below). According to [22, Sect. 1], let p_r be the minimum corank of any subgroup of Γ which lies in some algebraic subgroup of G of codimension r. In this section we shall prove some lower bounds for $p_1, ..., p_{n+1}$. It is easily verified that

$$p_r = \min_H \operatorname{corank}(\Gamma \cap H) \qquad (1 \leqslant r \leqslant n+1), \tag{11.1}$$

where H ranges over all algebraic subgroups of G of codimension r. We remark that we may assume that the minimum in (11.1) is taken over all

connected algebraic subgroups of G of codimension r. To see this, let H be a fixed algebraic subgroup of G of codimension r such that

$$\operatorname{corank}(\Gamma \cap H) = p_r, \tag{11.2}$$

let H^0 be the connected component of H, and let l be the index of H^0 in H. Then H^0 is a connected algebraic subgroup of G of codimension r since $\dim H^0 = \dim H$ (see Borel [9, pp. 86–88]). Hence

$$\operatorname{corank}(\Gamma \cap H^0) \geqslant p_r. \tag{11.3}$$

On the other hand, if elements $\alpha_1,.., \alpha_m$ of $\Gamma \cap H$ are linearly independent over $\mathbb{Z}$ then so are the elements $l\alpha_1,..., l\alpha_m$ of $\Gamma \cap H^0$. This observation together with (11.2) shows that

$$\operatorname{corank}(\Gamma \cap H^0) \leqslant p_r.$$

On combining this and (11.3) we get

$$\operatorname{corank}(\Gamma \cap H^0) = p_r. \tag{11.4}$$

Now the above remark follows from (11.4).

LEMMA 11.1. *Suppose H is a connected algebraic subgroup of $G = G_a^n \times E$. Then either $H = W \times E$ or $H = W \times \{\psi(0)\}$, where W is a subspace of the vector space $\mathbb{C}^n$ over $\mathbb{C}$.*

Proof. Let π_1', π_2' be the projections from G to G_a^n and E respectively. Let $i: H \to G$ be the embedding. Then $\pi_1 = \pi_1' \circ i: H \to G_a^n$ and $\pi_2 = \pi_2' \circ i: H \to E$ are homomorphisms of algebraic groups. Therefore $W = \pi_1(H)$ and $Y = \pi_2(H)$ are connected algebraic subgroups of G_a^n and E respectively. Thus W is a subspace of the vector space $\mathbb{C}^n$ over $\mathbb{C}$ (this fact can be shown by some elementary arguments; see also, for example, Kolchin [15]) and Y is either E or $\{\psi(0)\}$. We can also regard π_1, π_2 as surjective homomorphisms of algebraic groups from H to W and Y (with kernels N_1 and N_2) respectively. Then

$$N_1 = \{(0,..., 0)\} \times Y'$$

is an algebraic subgroups of H, so $Y' = \pi_2(N_1)$ is an algebraic subgroup of Y. Similarly

$$N_2 = W' \times \{\psi(0)\},$$

where W' is a subspace of W. We divide the proof into two cases according to whether $Y' = E$ or $Y' \neq E$. If $Y' = E$ then $\{(0,..., 0)\} \times E = N_1 \subseteq H$,

whence $W \times \{\psi(0)\} \subseteq H$. So $W \times E \subseteq H$. Further, $H \subseteq W \times E$ obviously. So $H = W \times E$. If $Y' \neq E$ then $\dim Y' = 0$ and the cardinal $|Y'|$ of Y' is finite. We assert that $Y \neq E$. For if $Y = E$ then there exist $\psi(z) \in E$ with finite order $m > |Y'|$ and $(a_1,..., a_n) \in W$ such that $(a_1,..., a_n) \times \psi(z) \in H$. Then

$$(m(a_1,..., a_n)) \times \psi(0) = m \cdot ((a_1,..., a_n) \times \psi(z)) \in H.$$

So $m(a_1,..., a_n) \in W'$, whence $(a_1,..., a_n) \in W'$. Thus $(a_1,..., a_n) \times \psi(0) \in W' \times \{\psi(0)\} = N_2 \subseteq H$. On combining this and $(a_1,..., a_n) \times \psi(z) \in H$, we get

$$(0,..., 0) \times \psi(z) \in H.$$

Hence $\psi(z) \in Y'$, a contradiction to the fact that $\psi(z)$ has order $m > |Y'|$. Thus the assertion $Y \neq E$ follows. Therefore $Y = \{\psi(0)\}$ and $H = W \times \{\psi(0)\}$. This completes the proof of Lemma 11.1.

We recall that Γ is an $\mathcal{O}$-module of rank $n+1$ over $\mathcal{O}$, which is generated by $\gamma_0,..., \gamma_n$ (see (9.7)) over $\mathcal{O}$. Let

$$\Gamma_a = \mathcal{O}^n + \mathcal{O}(\beta_1,..., \beta_n).$$

For any $\gamma_a = (\rho_1,..., \rho_n) + \rho_0(\beta_1,..., \beta_n)$, $\gamma_a' = (\rho_1',..., \rho_n') + \rho_0'(\beta_1,..., \beta_n)$ with $(\rho_0,..., \rho_n) \in \mathcal{O}^{n+1}$, $(\rho_0',..., \rho_n') \in \mathcal{O}^{n+1}$, and for any $\sigma \in \mathcal{O}$, we define

$$\gamma_a + \gamma_a' = (\rho_1 + \rho_1',..., \rho_n + \rho_n') + (\rho_0 + \rho_0')(\beta_1,..., \beta_n),$$
$$\sigma\gamma_a = (\sigma\rho_1,..., \sigma\rho_n) + (\sigma\rho_0)(\beta_1,..., \beta_n).$$

Then Γ_a becomes an $\mathcal{O}$-module. Note that Γ_a has rank $n+1$ over $\mathcal{O}$ by (5.2). For any $\mathcal{O}$-submodule Γ' of Γ we write $\operatorname{rank}_{\mathcal{O}} \Gamma'$ for its rank over $\mathcal{O}$. The same notation will be used for $\mathcal{O}$-submodules of Γ_a. Obviously

$$\operatorname{rank} \Gamma' = 2 \operatorname{rank}_{\mathcal{O}} \Gamma'. \tag{11.5}$$

Note that $\Gamma \cap H$ is an $\mathcal{O}$-submodule of Γ for any connected algebraic subgroup H of G by Lemma 11.1. Obviously, $\Gamma_a \cap W$ is an $\mathcal{O}$-submodule of Γ_a for any subspace W of $\mathbb{C}^n$.

LEMMA 11.2. *Let W be a subspace of the vector space $\mathbb{C}^n$ over $\mathbb{C}$. Then we have*

$$\operatorname{rank}_{\mathcal{O}}(\Gamma \cap (W \times \{\psi(0)\})) \leqslant 1, \tag{11.6}$$

and if $\dim W = v < n$ *then*

$$\operatorname{rank}_{\mathcal{O}}(\Gamma \cap (W \times E)) \leqslant v. \tag{11.7}$$

Proof. Write $\Gamma \cap (W \times \{\psi(0)\}) = \Delta$ and $\mathbf{0} = (0,\ldots, 0) \in \mathcal{O}^{n+1}$. To show (11.6), we treat two cases. If $\Delta = \{\gamma^{(\mathbf{0})}\}$ then $\operatorname{rank}_{\mathcal{O}} \Delta = 0$. If $\Delta \neq \{\gamma^{(\mathbf{0})}\}$, we can fix $\gamma^{(\boldsymbol{\rho})} \in \Delta$ with $\mathbf{0} \neq \boldsymbol{\rho} \in \mathcal{O}^{n+1}$. Let $\gamma^{(\boldsymbol{\sigma})}$ ($\boldsymbol{\sigma} \in \mathcal{O}^{n+1}$) be any non-zero element of Δ, so $\boldsymbol{\sigma} \neq \mathbf{0}$. Now $\psi(\boldsymbol{\rho} \cdot \mathbf{u}) = \psi(0)$, $\psi(\boldsymbol{\sigma} \cdot \mathbf{u}) = \psi(0)$ together with (5.1) give $0 \neq \boldsymbol{\rho} \cdot \mathbf{u} \in \mathscr{L}$ and $0 \neq \boldsymbol{\sigma} \cdot \mathbf{u} \in \mathscr{L}$. So there exist $m \in \mathbb{Z}$, $\alpha, \beta \in \mathcal{O}$ with $m\alpha\beta \neq 0$ such that

$$m\boldsymbol{\rho} \cdot \mathbf{u} = \alpha\omega_1, \qquad m\boldsymbol{\sigma} \cdot \mathbf{u} = \beta\omega_1. \tag{11.8}$$

By (11.8) and (5.1) we get $\rho'\boldsymbol{\rho} = \sigma'\boldsymbol{\sigma}$ with $0 \neq \rho' = m\beta \in \mathcal{O}$ and $0 \neq \sigma' = m\alpha \in \mathcal{O}$. Hence $\rho'\gamma^{(\boldsymbol{\rho})} = \sigma'\gamma^{(\boldsymbol{\sigma})}$. We conclude that $\operatorname{rank}_{\mathcal{O}} \Delta = 1$ in the case when $\Delta \neq \{\gamma^{(\mathbf{0})}\}$; (11.6) is thus established.

We now proceed to prove (11.7). Since $\pi: \gamma^{(\boldsymbol{\rho})} \to \gamma_a^{(\boldsymbol{\rho})} = (\rho_1 + \rho_0\beta_1,\ldots, \rho_n + \rho_0\beta_n)$ is an $\mathcal{O}$-module isomorphism from Γ to Γ_a by (5.2), and since $\pi(\Gamma \cap (W \times E)) = \Gamma_a \cap W$, we can regard π as an $\mathcal{O}$-module isomorphism from $\Gamma \cap (W \times E)$ to $\Gamma_a \cap W$. Hence

$$\operatorname{rank}_{\mathcal{O}}(\Gamma \cap (W \times E)) = \operatorname{rank}_{\mathcal{O}}(\Gamma_a \cap W). \tag{11.9}$$

Let

$$e_0 = (\beta_1,\ldots, \beta_n), \qquad e_1 = (1, 0,\ldots, 0),\ldots, e_n = (0,\ldots, 0, 1).$$

Denote by χ and χ_0 the canonical maps from $\mathbb{C}^n$ to $\mathbb{C}^n/W$ and Γ_a to $\Gamma_a/(\Gamma_a \cap W)$, respectively. Evidently, $\chi(e_1),\ldots, \chi(e_n)$ are a set of generators of $\mathbb{C}^n/W$ over $\mathbb{C}$. Let $t = \dim \mathbb{C}^n/W = n - v$, so $1 \leqslant t \leqslant n$. Without loss of generality, we can assume that $\chi(e_1),\ldots, \chi(e_t)$ are a basis of $\mathbb{C}^n/W$. Put $J = \{0, 1, 2,\ldots, n\}\backslash\{1, 2,\ldots, t\}$. To show (11.7) it suffices to verify the assertion that

$$\chi_0(e_{j_0}), \chi_0(e_1),\ldots, \chi_0(e_t) \qquad \text{are linearly independent over } \mathcal{O} \text{ for some } j_0 \in J, \tag{11.10}$$

for this implies that

$$n + 1 - \operatorname{rank}_{\mathcal{O}}(\Gamma_a \cap W) = \operatorname{rank}_{\mathcal{O}} \Gamma_a/(\Gamma_a \cap W) \geqslant t + 1,$$

whence

$$\operatorname{rank}_{\mathcal{O}}(\Gamma_a \cap W) \leqslant n - t = v,$$

which together with (11.9) yields (11.7). We now deduce a contradiction from the falsity of (11.10). Suppose (11.10) is false; i.e., for every $j \in J$

$$\chi_0(e_j), \chi_0(e_1),\ldots, \chi_0(e_t) \qquad \text{are linearly dependent over } \mathcal{O}.$$

Then for each $j \in J$ there exist $\rho_j, \rho_{j1}, \ldots, \rho_{jt}$ in $\mathscr{O}$ such that

$$\rho_j \chi_0(e_j) = \sum_{i=1}^{t} \rho_{ji} \chi_0(e_i), \qquad \rho_j \neq 0, \tag{11.11}$$

where $\rho_j \neq 0$ is implied by the linear independence of $\chi(e_1), \ldots, \chi(e_t)$ over $\mathbb{C}$. So we have

$$\rho_j \chi(e_j) = \sum_{i=1}^{t} \rho_{ji} \chi(e_i) \qquad (j \in J). \tag{11.12}$$

By (11.12) and $e_0 = \beta_1 e_1 + \cdots + \beta_n e_n$ we obtain

$$\chi(e_0) = \sum_{i=1}^{n} \beta_i \chi(e_i) = \sum_{i=1}^{t} \left(\beta_i + \sum_{j=t+1}^{n} (\rho_{ji}/\rho_j) \beta_j \right) \chi(e_i).$$

On combining this and (11.12) with $j = 0$, we get

$$\sum_{i=1}^{t} \left(-\rho_{0i}/\rho_0 + \beta_i + \sum_{j=t+1}^{n} (\rho_{ji}/\rho_j) \beta_j \right) \chi(e_i) = 0.$$

Hence, again by the linear independence of $\chi(e_1), \ldots, \chi(e_t)$ over $\mathbb{C}$, we obtain

$$-\rho_{0i}/\rho_0 + \beta_i + \sum_{j=t+1}^{n} (\rho_{ji}/\rho_j) \beta_j = 0 \qquad (1 \leqslant i \leqslant t),$$

a contradiction to (5.2). So (11.10) is established. This completes the proof of (11.7) and Lemma 11.2.

By (11.1) and (11.5) we have

$$\begin{aligned} p_r &= 2(n+1) - \max_H \operatorname{rank}(\Gamma \cap H) \\ &= 2(n+1) - 2 \max_H \operatorname{rank}_{\mathscr{O}}(\Gamma \cap H) \qquad (1 \leqslant r \leqslant n+1), \end{aligned} \tag{11.13}$$

where H ranges over all connected algebraic subgroups of G of codimension r. From (11.13) and Lemmas 11.1 and 11.2 it is easily seen, by some simple calculations, that the following lemma is valid.

LEMMA 11.3. *We have*

$$\begin{aligned} &p_r \geqslant 2(r+1) \qquad (1 \leqslant r \leqslant n-1), \\ &p_n \geqslant 2n, \\ &p_{n+1} = 2(n+1), \end{aligned} \tag{11.14}$$

where (11.14) *disappears in the case when* $n = 1$.

12. Preliminaries for the Algebraic Part

The following two lemmas were proved more generally in Brownawell and Masser [10] and in Masser [21], respectively, but for convenience we record them here.

Lemma 12.1. *Suppose that $\mathfrak{I}$ is a proper homogeneous ideal of $\mathfrak{R}$ of rank r satisfying $1 \leqslant r \leqslant N-1$, and let $P \in \mathfrak{R}$ be a homogeneous polynomial of degree $D \geqslant 1$ such that $\mathfrak{I} : (P) = \mathfrak{I}$. Then for the ideal $\mathfrak{L} = (\mathfrak{I}, P)$ we have*

$$\operatorname{rank} \mathfrak{L} = r + 1, \qquad \deg \mathfrak{L} = D \deg \mathfrak{I}.$$

Remark. The condition that P does not lie in any of the prime ideals of $\mathfrak{I}$ implies that $\mathfrak{I} : (P) = \mathfrak{I}$.

Lemma 12.2. *For an integer s with $1 \leqslant s \leqslant N+1$ let $P_1, \ldots, P_s$ be polynomials in $\mathfrak{R}$, and put $\mathfrak{I} = (P_1, \ldots, P_s)$. Then if $\mathfrak{I}^*$ is a non-zero proper ideal of $\mathfrak{R}$ it has rank at most s. Furthermore if $\mathfrak{I}^*$ has rank s it is unmixed.*

Recall the definition of the homogeneous prime ideal $\mathfrak{G}$ (see (9.6)). Let $t = 2n+1$ and

$$Q = Z_{02}^2 Z_{00} - 4Z_{01}^3 + g_2 Z_{00}^2 Z_{01} + g_3 Z_{00}^3, \quad f_0 = {}^aQ = y_2^2 - 4y_1^3 + g_2 y_1 + g_3. \tag{12.1}$$

Then

$$\operatorname{rank} \mathfrak{G} = t \tag{12.2}$$

(see [13, pp. 6, 11]). For later references we now show that

$${}^a\mathfrak{G} = (f_0). \tag{12.3}$$

By (9.6) we have ${}^a\mathfrak{G} \supseteq (f_0)$ since ${}^a\mathfrak{S} = (0)$. Further, ${}^a\mathfrak{G}$ is a prime ideal of rank $t - 2n = 1$ by Lemma 10.1, (7), (12.2), and the fact that $\mathfrak{G}$ is a homogeneous prime ideal containing $\mathfrak{S}$ and $Z_{00} \notin \mathfrak{G}$; (f_0) is also a prime ideal of rank 1 since f_0 is irreducible. Now (12.3) follows from these observations at once.

Lemma 12.3. *The degree of $\mathfrak{G}$ satisfies*

$$\deg \mathfrak{G} \leqslant 3 \cdot 4^n. \tag{12.4}$$

Furthermore there exist homogeneous polynomials $P_1, \ldots, P_t$ in $\mathfrak{R}$ such that the ideal $\mathfrak{I}_0 = (P_1, \ldots, P_t)$ satisfies $\mathfrak{I}_0^* = \mathfrak{G}$.

Proof. On applying [22, Lemma 5] to the variety $\varphi(\mathbb{P}^n \times \mathbb{P}^2) = Z(\mathfrak{S})$ and recalling that $\operatorname{rank} \mathfrak{S} = 2n$ and $\mathfrak{S}$ is generated by homogeneous polynomials of degree 2 (see (9.3)), we obtain

$$\deg \mathfrak{S} \leqslant 2^{2n} = 4^n.$$

On noting that $\mathfrak{S}$ is prime and $Q \notin \mathfrak{S}$, we see, by Lemma 12.1, that $\operatorname{rank}(\mathfrak{S}, Q) = 2n + 1 = t$, $\deg(\mathfrak{S}, Q) \leqslant 3 \cdot 4^n$. Since $\mathfrak{G} \supseteq (\mathfrak{S}, Q)$ by (9.6) and these both have rank t,

$$\deg \mathfrak{G} \leqslant \deg(\mathfrak{S}, Q) \leqslant 3 \cdot 4^n.$$

The second assertion of the lemma is a direct consequence of [22, Lemma 6].

For $f, g \in \mathfrak{R}_1$ we write

$$f \equiv g \pmod{f_0}$$

if $f - g \in (f_0)$. In Section 14 we need the following

LEMMA 12.4. *For any integers $i_1 \geqslant 0$, $i_2 \geqslant 0$ there exist polynomials $A_0(y_2), A_1(y_2) A_2(y_2)$ in $\mathbb{C}[y_2]$ with degrees at most $2i_1/3 + i_2 \leqslant i_1 + i_2$ such that*

$$y_1^{i_1} y_2^{i_2} \equiv A_0(y_2) y_1^2 + A_1(y_2) y_1 + A_2(y_2) \pmod{f_0}.$$

Proof. Without loss of generality, we may assume $i_2 = 0$. Write i for i_1. The case when $0 \leqslant i \leqslant 3$ is trivially true. Suppose that Lemma 12.4 holds for all i' with $0 \leqslant i' < i$ $(i > 3)$. Then there exist $B_j(y_2) \in \mathbb{C}[y_2]$ $(j = 0, 1, 2)$ with degrees at most $2(i-3)/3$ such that

$$\begin{aligned} y_1^i &= (1/4)\, y_1^{i-3} \cdot 4y_1^3 \\ &\equiv (B_0(y_2)\, y_1^2 + B_1(y_2) y_1 + B_2(y_2))(g_2 y_1 + y_2^2 + g_3), \pmod{f_0} \end{aligned} \tag{12.5}$$

since

$$4y_1^3 \equiv g_2 y_1 + y_2^2 + g_3 \pmod{f_0}. \tag{12.6}$$

From (12.5) we obtain, using (12.6) again, $A_j(y_2) \in \mathbb{C}[y_2]$ $(j = 0, 1, 2)$ with degrees at most $2(i-3)/3 + 2 = 2i/3$, such that

$$y_1^i \equiv A_0(y_2)\, y_1^2 + A_1(y_2)\, y_1 + A_2(y_2) \pmod{f_0}.$$

This completes the proof of Lemma 12.4.

LEMMA 12.5 (Masser). *Let Ω be an algebraically closed field of characteristic 0. For integers $l \geqslant n \geqslant 1$ and $D_1 \geqslant 1, \ldots, D_n \geqslant 1$ let $P_1, \ldots, P_l$ be polynomials in $\Omega[x_1, \ldots, x_n]$ with*

$$\deg_{x_i} P_j \leqslant D_i \qquad (1 \leqslant i \leqslant n, 1 \leqslant j \leqslant l).$$

Then if the ideal $(P_1, \ldots, P_l)$ is proper and non-zero, it has at most $n^n D_1 \cdots D_n$ isolated prime ideals of rank n.

Proof. The case when $D_1 = \cdots = D_n$ is given in [23, Sect. 2]. For the general case, see the Appendix.

For $m \geqslant 1$ we denote by $\mathbb{Z}^m$ the usual additive group of elements $v = (s_1, \ldots, s_m)$ for $s_i \in \mathbb{Z}$ $(1 \leqslant i \leqslant m)$. For real numbers $S_1 \geqslant 0, \ldots, S_m \geqslant 0$ we denote by $\mathbb{Z}^m(S_1, \ldots, S_m)$ the subset of $\mathbb{Z}^m$ consisting of elements $v = (s_1, \ldots, s_m)$ with $0 \leqslant s_1 \leqslant S_1, \ldots, 0 \leqslant s_m \leqslant S_m$.

The following lemma is a modification of [21, Lemma 3].

LEMMA 12.6. *Suppose for some real $S_1, \ldots, S_m$ with $0 \leqslant S_1 \leqslant \cdots \leqslant S_m$ there is an equivalence relation on $\mathbb{Z}^m(S_1, \ldots, S_m)$ with B equivalence classes. If*

$$S_1 \cdots S_{m+1-q} \geqslant B$$

for some integer q with $1 \leqslant q \leqslant m$, then there are elements $v_1, v_1', \ldots, v_q, v_q'$ of $\mathbb{Z}^m(S_1, \ldots, S_m)$ such that v_i' is equivalent to v_i $(1 \leqslant i \leqslant q)$ and the differences $v_1' - v_1, \ldots, v_q' - v_q$ are linearly independent over $\mathbb{Z}$.

Proof. We proceed in a way similar to the proof of [21, Lemma 3]. A subgroup U of $\mathbb{Z}^m$ is called a coordinate subgroup if it is defined by the vanishing of a (possibly empty) subset of the m coordinates. Such an U is clearly divisible; i.e., if $lv \in U$ for some $0 \neq l \in \mathbb{Z}$ and $v \in \mathbb{Z}^m$, then $v \in U$. Write $U(S_1, \ldots, S_m) = U \cap \mathbb{Z}^m(S_1, \ldots, S_m)$ and $U_0 = \mathbb{Z}^m(S_1, \ldots, S_m)$. We assert that there exist coordinate subgroups $U_1, \ldots, U_q$ and elements $v_1, v_1', \ldots, v_q, v_q'$ of $\mathbb{Z}^m(S_1, \ldots, S_m)$ such that $U_{i-1} \supset U_i$, the rank of U_i is $m - i$, the elements v_i, v_i' are equivalent, and the differences $v_i' - v_i$ lie in U_{i-1} but not in U_i $(1 \leqslant i \leqslant q)$. This assertion can be proved by some modifications of the arguments in [21, Lemma 3]; i.e., replace $\mathbb{Z}^h$, $\mathbb{Z}^h(N)$, and $U_r(N)$, $1 \leqslant r \leqslant k-1$, by $\mathbb{Z}^m$, $\mathbb{Z}^m(S_1, \ldots, S_m)$, and $U_r(S_1, \ldots, S_m)$, $1 \leqslant r \leqslant q-1$, respectively, and replace (2), (3) in [21, Lemma 3] by the assertions that $\mathbb{Z}^m(S_1, \ldots, S_m)$ contains

$$([S_1] + 1) \cdots ([S_m] + 1) > S_1 \cdots S_m \geqslant B$$

elements and that $U_r(S_1,\dots,S_m)$ contains at least

$$([S_1]+1)\cdots([S_{m-r}]+1)\geqslant([S_1]+1)\cdots([S_{m+1-q}]+1)$$
$$>S_1\cdots S_{m+1-q}\geqslant B$$

elements, respectively.

The linear independence over $\mathbb{Z}$ of $v_1'-v_1,\dots,v_q'-v_q$ is implied by the above constructions and the divisibility of the coordinate subgroups.

The proof of Lemma 12.6 is thus complete.

For an integer r with $1\leqslant r\leqslant n+1$, let

$$p_r'=\min(p_r,p_{r+1},\dots,p_{n+1})\qquad(1\leqslant r\leqslant n+1)$$

and let q_r be the minimum corank of any subgroup Δ of the additive group $\mathscr{O}^{n+1}$ for which there exists a special homogeneous prime ideal $\mathfrak{P}$ of rank $t+r=\operatorname{rank}\mathfrak{G}+r$, such that $\mathscr{E}(\delta)\mathfrak{P}=\mathfrak{P}$ for all $\delta\in\Delta$, i.e., $S(\mathfrak{P})\supseteq\Delta$. On recalling that $\rho\to\gamma^{(\rho)}$ is a group isomorphism from $\mathscr{O}^{n+1}$ to Γ, [22, p. 502, (23)] and our Lemma 11.3 imply that

$$\begin{aligned}&q_r\geqslant p_r'\geqslant 2(r+1)&&(1\leqslant r\leqslant n-1),\\&q_n\geqslant p_n'\geqslant 2n,\\&q_{n+1}\geqslant p_{n+1}'=2(n+1),&&\text{i.e., } q_{n+1}=2(n+1),\end{aligned}\tag{12.7}$$

where the first row (in (12.7)) disappears in the case when $n=1$.

13. The Inductive Lemma: The First n Steps

For any real $R_0\geqslant 0,\dots,R_n\geqslant 0$ denote by $\mathscr{O}^{n+1}(R_0,\dots,R_n)$ the set of $\rho=(\rho_0,\dots,\rho_n)\in\mathscr{O}^{n+1}$ with $\rho_i\in\mathscr{O}(R_i)$ $(0\leqslant i\leqslant n)$ and denote by $\Gamma(R_0,\dots,R_n)$ the set of elements $\gamma^{(\rho)}\in\Gamma$ for all $\rho\in\mathscr{O}^{n+1}(R_0,\dots,R_n)$. Let

$$\begin{aligned}&\mathscr{O}_0=\mathscr{O}^{n+1}(S_0/(n+1),\dots,S_n/(n+1)),\\&\Gamma_i=\Gamma\left(\left(1-\frac{i}{n+1}\right)S_0,\dots,\left(1-\frac{i}{n+1}\right)S_n\right)\qquad(0\leqslant i\leqslant n+1).\end{aligned}\tag{13.1}$$

Obviously

$$\{(0,\dots,0)\times\psi(0)\}=\Gamma_{n+1}\subseteq\Gamma_n\subseteq\cdots\subseteq\Gamma_1\subseteq\Gamma_0=\Gamma(S_0,\dots,S_n).\tag{13.2}$$

Suppose now Proposition 5.1 is false. That is, there exists a polynomial $0\neq P(x_1,\dots,x_n,y)\in\mathbb{C}[x_1,\dots,x_n,y]$ satisfying (5.8) and (5.9) (for later convenience, we shall write y_1 for y). Then we proceed to prove the following

Inductive Lemma, from which we shall deduce a contradiction and Proposition 5.1 will be established by this contradiction.

Recall $L_0 = [L]$, $M_0 = [M]$, rank $\mathfrak{G} = 2n + 1 = t$, and $\mathfrak{I}_0 = (P_1, ..., P_t)$ is the ideal in Lemma 12.3 so that $\mathfrak{I}_0^* = \mathfrak{G} = I(G)$ (see (9.6)), whence $\mathfrak{I}_0$ vanishes on G.

For later convenience, for any $f \in \mathfrak{R}_1 = \mathbb{C}[x_1, ..., x_n, y_1, y_2]$ we denote by $\deg_x f$ and $\deg_y f$ the total degrees of f in $x_1, ..., x_n$ and y_1, y_2, respectively.

INDUCTIVE LEMMA. *Let r be an integer with $1 \leqslant r \leqslant n + 2$. Then there exist homogeneous polynomials $P_{t+1}, ..., P_{t+r}$ in $\mathfrak{R}$ such that*

(i) *for $r < n + 2$ and $1 \leqslant i \leqslant r$, $\deg P_{t+i} = nL_0$, $\deg_{x_j} {}^a P_{t+i} \leqslant L_0$ $(1 \leqslant j \leqslant n)$, $\deg_y {}^a P_{t+i} \leqslant 2^{i-1} M_0$;*

(ii) *$\mathfrak{I}_r = (P_1, ..., P_t, P_{t+1}, ..., P_{t+r})$ vanishes on Γ_{r-1};*

(iii) *rank $\mathfrak{I}_r^* = t + r$;*

(iv) *for $1 \leqslant r \leqslant n$, $\deg \mathfrak{I}_r^* \leqslant 3 \cdot 4^n (nL_0)^r$;*

(v) *the number of bad prime ideals of $\mathfrak{I}_n^*$ is at most $3 \cdot 4^{n-1}(n+1)^{n+1} L_0^{n-1} M_0$;*

(vi) *the number of prime ideals of $\mathfrak{I}_{n+1}^*$ is at most $3 \cdot 2^n (n+2)^{n+2} L_0^n M_0$.*

Proof of (i)–(iii) *for $1 \leqslant r \leqslant n$ and of* (iv).

We proceed by induction on r.

For $r = 1$, we set

$$P_{t+1} = Z_{00}^d {}^h P,$$

where $d \geqslant 0$ is an integer such that $\deg P_{t+1} = nL_0$ (by (5.4) such d does exist). Condition (i) holds by ${}^a P_{t+1} = P$ and (5.8), and (ii) follows from the fact, which is implied by (5.9), that P_{t+1} vanishes on Γ_0 and the fact that $\mathfrak{I}_0 = (P_1, ..., P_t)$ vanishes on $G \supset \Gamma_0$. To show (iii) and (iv) set $\mathfrak{I} = (\mathfrak{I}_0^*, P_{t+1}) = (\mathfrak{G}, P_{t+1})$. We assert that $P_{t+1} \notin \mathfrak{G}$, for otherwise we should have $P = {}^a P_{t+1} \in {}^a \mathfrak{G} = (y_2^2 - 4y_1^3 + g_2 y_1 + g_3)$ by (12.3), and this contradicts the fact that $P \neq 0$ and $\deg_{y_2} P = 0$. Thus, by Lemmas 12.1 and 12.3, we have

$$\text{rank } \mathfrak{I} = \text{rank } \mathfrak{G} + 1 = t + 1,$$

$$\deg \mathfrak{I} = \deg P_{t+1} \cdot \deg \mathfrak{G} \leqslant 3 \cdot 4^n n L_0.$$

Now

$$\mathfrak{I}_1^* = (\mathfrak{I}_0, P_{t+1})^* \supseteq (\mathfrak{I}_0^*, P_{t+1}) = \mathfrak{I},$$

so rank $\mathfrak{I}_1^* \geqslant \text{rank } \mathfrak{I} = t + 1$. On the other hand rank $\mathfrak{I}_1^* \leqslant t + 1$ by

Lemma 12.2 and the fact that $\mathfrak{I}_1^* \neq \mathfrak{R}$ since $\mathfrak{I}_1^*$ vanishes on Γ_0. Hence rank $\mathfrak{I}_1^* = t+1$. Furthermore

$$\deg \mathfrak{I}_1^* \leqslant \deg \mathfrak{I} \leqslant 3 \cdot 4^n nL_0.$$

This completes the proof for the case $r = 1$.

If $n = 1$ there is nothing more to prove for proving (i)–(iii) for $1 \leqslant r \leqslant n$ and (iv). So we suppose that $n \geqslant 2$ and (i)–(iv) have been verified for some r with $1 \leqslant r \leqslant n-1$. We start by constructing the appropriate polynomial P_{t+r+1}. Then we verify (i)–(iv) for $r+1$.

Since rank $\mathfrak{I}_r^* = t+r$, the ideal $\mathfrak{I}_r^*$ is unmixed by Lemma 12.2. Hence every prime ideal of $\mathfrak{I}_r^*$ is of rank $t+r$. Choose an arbitrary such prime ideal $\mathfrak{P}$ to be fixed in the next few paragraphs.

We first prove that

$$\mathscr{E}(\boldsymbol{\rho})\,\mathfrak{I}_r^* \not\subseteq \mathfrak{P} \tag{13.3}$$

for some $\boldsymbol{\rho} \in \mathscr{O}_0 = \mathscr{O}^{n+1}(S_0/(n+1),\ldots, S_n/(n+1))$. If (13.3) is false, then

$$\mathscr{E}(\boldsymbol{\rho})\,\mathfrak{I}_r^* \subseteq \mathfrak{P} \qquad \text{for all } \boldsymbol{\rho} \in \mathscr{O}_0. \tag{13.4}$$

Note that $\mathfrak{I}_r^*$, and therefore $\mathfrak{P}$, are special homogeneous ideals in the sense of Section 9, since $\mathfrak{G} = \mathfrak{I}_0^* \subseteq \mathfrak{I}_r^* \subseteq \mathfrak{P}$ and $(\mathfrak{I}_r^*)^* = \mathfrak{I}_r^*$, $\mathfrak{P}^* = \mathfrak{P}$. On applying $\mathscr{E}(-\boldsymbol{\rho})$ to (13.4), we deduce that $\mathfrak{I}_r^* \subseteq \mathscr{E}(-\boldsymbol{\rho})\mathfrak{P}$ by Lemma 9.4. By Lemma 9.5, $\mathscr{E}(-\boldsymbol{\rho})\mathfrak{P}$ is prime of rank $t+r$. Thus $\mathscr{E}(-\boldsymbol{\rho})\mathfrak{P}$ is a prime ideal of $\mathfrak{I}_r^*$ for every $\boldsymbol{\rho} \in \mathscr{O}_0$.

We now define an equivalence relation on

$$\mathbb{Z}_0 = \mathbb{Z}^{2(n+1)}(S_0/(n+1), S_0/(n+1),\ldots, S_n/(n+1), S_n/(n+1)). \tag{13.5}$$

There is an isomorphism T from $\mathbb{Z}^{2(n+1)}$ to $\mathscr{O}^{n+1}$ which sends $v = (r_0, s_0,\ldots, r_n, s_n) \in \mathbb{Z}^{2(n+1)}$ to $\boldsymbol{\rho} = (r_0 + s_0\tau,\ldots, r_n + s_n\tau) \in \mathscr{O}^{n+1}$. Clearly $T(\mathbb{Z}_0) = \mathscr{O}_0$. We say that the elements v, v' of $\mathbb{Z}_0$ are equivalent if the elements $\boldsymbol{\rho} = T(v)$, $\boldsymbol{\rho}' = T(v')$ of $\mathscr{O}_0$ satisfy $\mathscr{E}(-\boldsymbol{\rho})\mathfrak{P} = \mathscr{E}(-\boldsymbol{\rho}')\mathfrak{P}$; i.e., on recalling (10.18), $\boldsymbol{\rho}' - \boldsymbol{\rho} \in S(\mathfrak{P})$. The number B of the equivalence classes does not exceed the number of prime ideals of $\mathfrak{I}_r^*$. The latter number is at most $\deg \mathfrak{I}_r^*$, since $\mathfrak{I}_r^*$ is unmixed. Thus we have

$$B \leqslant 3 \cdot 4^n (nL_0)^r,$$

by the inductive hypothesis (iv). So by (5.5) we can apply Lemma 12.6 with $q = 2(n+1) + 1 - 2(r+1)$ to $\mathbb{Z}_0$ and the equivalence relation defined above, and therefore see that there exist q pairs of elements $v_1, v_1',\ldots, v_q, v_q'$ of $\mathbb{Z}_0$ such that v_i' is equivalent to v_i $(1 \leqslant i \leqslant q)$ and $v_1' - v_1,\ldots, v_q' - v_q$ are linearly independent over $\mathbb{Z}$. Let $\boldsymbol{\rho}^{(i)} = T(v_i' - v_i)$ $(1 \leqslant i \leqslant q)$. Then $\boldsymbol{\rho}^{(1)},\ldots, \boldsymbol{\rho}^{(q)}$ lie in

$S(\mathfrak{P})$ and are linearly independent over $\mathbb{Z}$. Hence corank $S(\mathfrak{P}) \leqslant 2(n+1)-q = 2(r+1)-1$.

On the other hand, by the definition of q_r (see Section 12) and (12.7), we have corank $S(\mathfrak{P}) \geqslant q_r \geqslant 2(r+1)$. We have thus deduced a contradiction, by which (13.3) is established.

Hence there exists $\boldsymbol{\rho} \in \mathscr{O}_0$ such that

$$\mathscr{E}(\boldsymbol{\rho})\, \mathfrak{I}_r^* \not\subseteq \mathfrak{P}.$$

It follows that

$$E(\boldsymbol{\rho})\, \mathfrak{I}_r^* \not\subseteq \mathfrak{P}, \tag{13.6}$$

where $E(\boldsymbol{\rho})$ is defined in Section 9. For otherwise we should have

$$\mathscr{E}(\boldsymbol{\rho})\, \mathfrak{I}_r^* = (E(\boldsymbol{\rho})\, \mathfrak{I}_r^*, \mathfrak{G})^* \subseteq (\mathfrak{P}, \mathfrak{G})^* = \mathfrak{P}^* = \mathfrak{P}.$$

We now assert that

$$E(\boldsymbol{\rho})\, \mathfrak{I}_r \not\subseteq \mathfrak{P}. \tag{13.7}$$

For (13.6) implies that there exists $R \in \mathfrak{I}_r^*$ such that $E(\boldsymbol{\rho})R \notin \mathfrak{P}$. There also is $R_1 \in \mathscr{M}$ such that $R_1 R \in \mathfrak{I}_r$. Since $E(\boldsymbol{\rho})\, R_1 \in \mathscr{M}$ (by Lemma 9.3) and $\mathfrak{P} \cap \mathscr{M} = \varnothing$ we have $E(\boldsymbol{\rho})\, R_1 \notin \mathfrak{P}$. Hence $E(\boldsymbol{\rho})(R_1 R) = E(\boldsymbol{\rho})\, R_1 \cdot E(\boldsymbol{\rho})R \notin \mathfrak{P}$. This verifies (13.7).

Since $\mathfrak{I}_r = (P_1, \ldots, P_{t+r})$ it follows from (13.7) that

$$E(\boldsymbol{\rho})\, P_j \notin \mathfrak{P} \tag{13.8}$$

for some j with $1 \leqslant j \leqslant t+r$. In fact we have $j \geqslant t+1$, since for $1 \leqslant i \leqslant t$ we have $E(\boldsymbol{\rho})\, P_i \in E(\boldsymbol{\rho})\, \mathfrak{G} \subseteq \mathfrak{G} \subseteq \mathfrak{P}$ by Lemma 9.3.

Let $d_1 = \deg_x {}^a P_j$, $d_2 = \deg_y {}^a P_j$, $d = \max(d_1, d_2)$. Then by the inductive hypothesis (i) and (5.4)

$$\deg P_j = nL_0, \qquad d_1 \leqslant nL_0, \qquad d_2 \leqslant 2^{r-1} M_0, \qquad d \leqslant nL_0. \tag{13.9}$$

By (10.5) and (13.9) we obtain

$${}^a(E(\boldsymbol{\rho})\, P_j) = H_{\boldsymbol{\rho}}^{d'} f \qquad \text{with} \quad d' = nL_0 - d_2 \geqslant 0, \tag{13.10}$$

where

$$f = H_{\boldsymbol{\rho}}^{d_2}\, {}^a P_j(x_1 + \rho_1 + \rho_0\beta_1, \ldots, x_n + \rho_n + \rho_0\beta_n, F_{\boldsymbol{\rho}}/H_{\boldsymbol{\rho}}, G_{\boldsymbol{\rho}}/H_{\boldsymbol{\rho}}) \tag{13.11}$$

is a polynomial in $\mathfrak{R}_1$. By (13.9), (13.11) we have

$$\deg_{x_i} f \leqslant L_0, \qquad \deg_y f \leqslant 2^r M_0. \tag{13.12}$$

Hence ${}^hf \in \mathfrak{R}$ is homogeneous of degree $d'' \leqslant nL_0$ by (5.4). Set

$$Q_{\mathfrak{P}} = Z_{00}^{nL_0 - d''}\, {}^hf. \tag{13.13}$$

Then $Q_{\mathfrak{P}}$ is homogeneous with

$$\deg Q_{\mathfrak{P}} = nL_0, \qquad \deg_{x_i} {}^aQ_{\mathfrak{P}} \leqslant L_0, \qquad \deg_y {}^aQ_{\mathfrak{P}} \leqslant 2^r M_0 \tag{13.14}$$

by (13.12) and (10.3). We now prove that

$$Q_{\mathfrak{P}} \notin \mathfrak{P} \tag{13.15}$$

and

$$Q_{\mathfrak{P}} \text{ vanishes on } \Gamma_r. \tag{13.16}$$

It follows from (10.4) and (13.10) that

$$Z_{00}^{m_1}\, {}^{ha}(E(\mathbf{p})\, P_j) - ({}^hH_{\mathbf{p}})^{d'}\, {}^hf \in \mathfrak{S}$$

for some integer $m_1 \geqslant 0$. Hence by (10.6) there is an integer $m_2 \geqslant 0$ such that

$$Z_{00}^{m_1} E(\mathbf{p})\, P_j - Z_{00}^{m_2} ({}^hH_{\mathbf{p}})^{d'}\, {}^hf \in \mathfrak{S} \subseteq \mathfrak{P}. \tag{13.17}$$

Now (13.8) gives $Z_{00}^{m_1} E(\mathbf{p})\, P_j \notin \mathfrak{P}$ since $Z_{00} \notin \mathfrak{P}$. This together with (13.17) and ${}^hH_{\mathbf{p}} \notin \mathfrak{P}$ (since ${}^hH_{\mathbf{p}} \in \mathscr{M}$ by Lemma 9.1) implies that ${}^hf \notin \mathfrak{P}$, and therefore (13.15) follows by (13.13).

Since by the inductive hypothesis (ii), $\mathfrak{I}_r$, and therefore $\mathfrak{I}_r^*$, vanish on Γ_{r-1}, Lemma 9.5 and the fact that $\mathbf{p} \in \mathscr{C}_0$ imply that $\mathscr{E}(\mathbf{p})\, \mathfrak{I}_r^*$ vanishes on Γ_r. Hence the polynomial $E(\mathbf{p})\, P_j \in \mathscr{E}(\mathbf{p})\, \mathfrak{I}_r^*$ vanishes on Γ_r. On combining this observation and (13.17), recalling $\mathfrak{S} \subseteq \mathfrak{G} = I(G)$ and the fact that Z_{00} and ${}^hH_{\mathbf{p}}$ are in $\mathscr{M}$, we conclude that ${}^hf$ vanishes on Γ_r and therefore (13.16) follows by (13.13).

Thus for each prime ideal $\mathfrak{P}$ of $\mathfrak{I}_r^*$ we have constructed a homogeneous polynomial $Q_{\mathfrak{P}} \in \mathfrak{R}$ satisfying (13.14)–(13.16). By (13.15) and [10, Lemma 5] there exists for each prime ideal $\mathfrak{P}$ of $\mathfrak{I}_r^*$ a constant $\lambda_{\mathfrak{P}} \in \mathbb{C}$ such that

$$P_{t+r+1} = \sum \lambda_{\mathfrak{P}} Q_{\mathfrak{P}} \notin \mathfrak{P}' \tag{13.18}$$

for any prime ideal $\mathfrak{P}'$ of $\mathfrak{I}_r^*$, where the sum is taken over all prime ideals $\mathfrak{P}$ of $\mathfrak{I}_r^*$. Obviously, P_{t+r+1} is homogeneous by (13.14). Now (i), (ii) for $r+1$ follow from the inductive hypotheses (i), (ii), the definition (13.18) of P_{t+r+1}, (13.14), (13.16), and (13.2). It remains to verify (iii) and (iv) for

$r+1$. Let $\mathfrak{I}' = (\mathfrak{I}_r^*, P_{t+r+1})$. Then (13.18) and the inductive hypotheses (iii), (iv) imply, by Lemma 12.1, that

$$\operatorname{rank} \mathfrak{I}' = \operatorname{rank} \mathfrak{I}_r^* + 1 = t + r + 1, \tag{13.19}$$

$$\deg \mathfrak{I}' = \deg P_{t+r+1} \cdot \deg \mathfrak{I}_r^* \leqslant 3 \cdot 4^n (nL_0)^{r+1}. \tag{13.20}$$

Since $\mathfrak{I}_{r+1}^* = (\mathfrak{I}_r, P_{t+r+1})^* \supseteq \mathfrak{I}'$, (13.19) yields $\operatorname{rank} \mathfrak{I}_{r+1}^* \geqslant t + r + 1$. On the other hand, noting that $\mathfrak{I}_{r+1}^* \neq \mathfrak{R}$ (since $\mathfrak{I}_{r+1}$, and therefore $\mathfrak{I}_{r+1}^*$, vanish on Γ_r), Lemma 12.2 implies that $\operatorname{rank} \mathfrak{I}_{r+1}^* \leqslant t + r + 1$. Hence $\operatorname{rank} \mathfrak{I}_{r+1}^* = t + r + 1$; i.e., (iii) for $r+1$ is verified. Furthermore since $\mathfrak{I}_{r+1}^* \supseteq \mathfrak{I}'$ and these have the same rank, we obtain $\deg \mathfrak{I}_{r+1}^* \leqslant \deg \mathfrak{I}' \leqslant 3 \cdot 4^n (nL_0)^{r+1}$ by (13.20); i.e., (iv) for $r+1$ is proved. Thus we have completed the inductive proof of (i)–(iii) for $1 \leqslant r \leqslant n$ and the inductive proof of (iv).

14. The Final Two Steps; the Proof of Proposition 5.1 (Completion)

Proof of the Inductive Lemma (Completion). We first prove (v). Let

$$\mathfrak{A} = (\mathfrak{G}, P_{t+1}, \ldots, P_{t+n}). \tag{14.1}$$

Obviously $\mathfrak{A}$ is homogeneous. Recalling $(P_1, \ldots, P_t)^* = \mathfrak{I}_0^* = \mathfrak{G}$ (see Lemma 12.3) and $\mathfrak{I}_n = (P_1, \ldots, P_t, P_{t+1}, \ldots, P_{t+n})$, it is easily seen that $\mathfrak{I}_n \subseteq \mathfrak{A} \subseteq \mathfrak{I}_n^*$, whence $\mathfrak{I}_n^* \subseteq \mathfrak{A}^* \subseteq (\mathfrak{I}_n^*)^* = \mathfrak{I}_n^*$, i.e.,

$$\mathfrak{I}_n^* = \mathfrak{A}^*. \tag{14.2}$$

Suppose that

$$\mathfrak{A} = \bigcap_i \mathfrak{Q}_i \qquad (\sqrt{\mathfrak{Q}_i} = \mathfrak{P}_i) \tag{14.3}$$

is an irredundant primary representation, all $\mathfrak{Q}_i$, and therefore $\mathfrak{P}_i$, being homogeneous (see [30, Vol. II, p. 153, Theorem 9]). If all prime ideals of $\mathfrak{I}_n^*$ are good, (v) is trivial. So by (14.2), (14.3), and [30, Vol. I, p. 225, Theorem 17] we can assume that there exists a subset $J \neq \varnothing$ of the indices i such that $j \in J$ if and only if $\mathfrak{P}_j$ is a bad prime ideal of $\mathfrak{I}_n^*$.

For each $j \in J$, $\mathfrak{P}_j$ is special, with

$$\operatorname{rank} \mathfrak{P}_j = \operatorname{rank} \mathfrak{I}_n^* = t + n, \tag{14.4}$$

since $\mathfrak{I}_n^*$ is unmixed by (iii) for $r = n$ and Lemma 12.2. Evidently, $\mathfrak{P}_j$ is an isolated prime ideal of $\mathfrak{A}$, since $\mathfrak{A}^* = \mathfrak{I}_n^*$ is unmixed and $\mathfrak{P}_j$ is a prime ideal of $\mathfrak{A}^*$.

By Lemma 10.1, we see that

$$ {}^{a}\mathfrak{A} = \bigcap_{i'} {}^{a}\mathfrak{Q}_{i'} \qquad (\sqrt{{}^{a}\mathfrak{Q}_{i'}} = {}^{a}\mathfrak{P}_{i'}), \tag{14.5} $$

where i' ranges over all i with $Z_{00} \notin \mathfrak{P}_i$, is an irredundant primary representation. Note that ${}^{a}\mathfrak{P}_j$ is a prime ideal of ${}^{a}\mathfrak{A}$ (i.e., J is also a subset of the set of the indices i'), since $\mathfrak{P}_j$ is special whence $Z_{00} \notin \mathfrak{P}_j$. Further, we assert that ${}^{a}\mathfrak{P}_j$ is isolated. For ${}^{a}\mathfrak{P}_{i'} \subseteq {}^{a}\mathfrak{P}_j$ implies, by (10.10), that $\mathfrak{P}_{i'} = {}^{ha}\mathfrak{P}_{i'} \subseteq {}^{ha}\mathfrak{P}_j = \mathfrak{P}_j$. This yields, since $\mathfrak{P}_j$ is an isolated prime ideal of $\mathfrak{A}$, that $\mathfrak{P}_{i'} = \mathfrak{P}_j$, and therefore ${}^{a}\mathfrak{P}_{i'} = {}^{a}\mathfrak{P}_j$.

By Lemma 10.2, there exists a linear form

$$ \zeta = a_1 x_1 + \cdots + a_n x_n \neq 0 $$

with $a_i \in \mathbb{C}$ $(1 \leqslant i \leqslant n)$ such that

$$ {}^{a}\mathfrak{P}_j \cap \mathbb{C}[\zeta] = (0) \qquad (j \in J). \tag{14.6} $$

Without loss of generality, we may assume $a_1 \neq 0$. Let

$$ \mathscr{M}_1 = \mathbb{C}[\zeta] \backslash \{0\}. $$

Then $\mathscr{M}_1$ is a multiplicative set in $\mathfrak{R}_1 = \mathbb{C}[x_1, \ldots, x_n, y_1, y_2]$. Denote by $(\mathfrak{R}_1)_{\mathscr{M}_1}$ the quotient ring of $\mathfrak{R}_1$ with respect to $\mathscr{M}_1$. For an ideal $\mathfrak{a}$ in $\mathfrak{R}_1$, write $\mathfrak{a}^e$ for the extended ideal, and write $\mathfrak{a}^{ec}$ for the contracted extension with respect to $\mathscr{M}_1$. By [30, Vol. I, p. 225, Theorem 17],

$$ ({}^{a}\mathfrak{A})^e = \bigcap_{i''} ({}^{a}\mathfrak{Q}_{i''})^e, \qquad \sqrt{({}^{a}\mathfrak{Q}_{i''})^e} = ({}^{a}\mathfrak{P}_{i''})^e, \tag{14.7} $$

where i'' ranges over all i' with ${}^{a}\mathfrak{P}_{i'} \cap \mathscr{M}_1 = \varnothing$, is an irredundant primary representation. It follows from (14.6) that $({}^{a}\mathfrak{P}_j)^e$ is a prime ideal of $({}^{a}\mathfrak{A})^e$ for all $j \in J$; i.e., J is a subset of the set of the indices i''. We assert further that $({}^{a}\mathfrak{P}_j)^e$ is isolated for all $j \in J$. For $({}^{a}\mathfrak{P}_{i''})^e \subseteq ({}^{a}\mathfrak{P}_j)^e$ implies, by [30, Vol. I, p. 225, Theorem 17], that ${}^{a}\mathfrak{P}_{i''} = ({}^{a}\mathfrak{P}_{i''})^{ec} \subseteq ({}^{a}\mathfrak{P}_j)^{ec} = {}^{a}\mathfrak{P}_j$. This yields, since ${}^{a}\mathfrak{P}_j$ is an isolated prime ideal of ${}^{a}\mathfrak{A}$, that ${}^{a}\mathfrak{P}_{i''} = {}^{a}\mathfrak{P}_j$, therefore $({}^{a}\mathfrak{P}_{i''})^e = ({}^{a}\mathfrak{P}_j)^e$. Moreover, by [30, Vol. I, p. 224, Theorem 16, Corollary 1], Lemma 10.1, and (14.4), we have

$$ \operatorname{rank}({}^{a}\mathfrak{P}_j)^e = \operatorname{rank} {}^{a}\mathfrak{P}_j = \operatorname{rank} \mathfrak{P}_j - 2n = n + 1. $$

Thus, summing up, we have proved that

$$ ({}^{a}\mathfrak{P}_j)^e \text{ is an isolated prime ideal of } ({}^{a}\mathfrak{A})^e \text{ of rank } n + 1 \ (j \in J). \tag{14.8} $$

We now observe that

$$(\mathfrak{R}_1)_{\mathscr{M}_1} = \mathbb{C}(\zeta)[x_2,..., x_n, y_1, y_2] \qquad (= \mathfrak{R}_3, \text{ say}) \tag{14.9}$$

by $a_1 \neq 0$. Further, by (12.3) and (14.1) we have

$${}^a\mathfrak{A} = (f_0, {}^aP_{t+1},..., {}^aP_{t+n}), \tag{14.10}$$

where $f_0 = y_2^2 - 4y_1^3 + g_2 y_1 + g_3$ (see (12.1)). By Lemma 12.4 and (i) for $r = n$, there exist $f_1,..., f_n$ in $\mathfrak{R}_1$ satisfying

$${}^aP_{t+m} \equiv f_m \pmod{f_0} \qquad (1 \leqslant m \leqslant n) \tag{14.11}$$

and

$$\deg_{x_l} f_m \leqslant L_0, \quad \deg_{y_1} f_m \leqslant 2, \quad \deg_{y_2} f_m \leqslant 2^{n-1}M_0 \quad (2 \leqslant l \leqslant n, 1 \leqslant m \leqslant n). \tag{14.12}$$

By (14.10), (14.11) we get

$${}^a\mathfrak{A} = (f_0, f_1,..., f_n). \tag{14.13}$$

On substituting $(1/a_1)(\zeta - a_2x_2 - \cdots - a_nx_n)$ for x_1, we can rewrite $f_1,..., f_n$ as

$$f_m(x_1,..., x_n, y_1, y_2) = \psi_m(\zeta, x_2,..., x_n, y_1, y_2) \in \mathfrak{R}_3 \qquad (1 \leqslant m \leqslant n). \tag{14.14}$$

It follows from (14.12) that

$$\deg_{x_l} \psi_m \leqslant 2L_0, \quad \deg_{y_1} \psi_m \leqslant 2, \quad \deg_{y_2} \psi_m \leqslant 2^{n-1}M_0 \quad (2 \leqslant l \leqslant n, \ 1 \leqslant m \leqslant n). \tag{14.15}$$

We see from (14.13) and (14.14) that $({}^a\mathfrak{A})^e$ is an ideal of $\mathfrak{R}_3$ generated by $f_0, \psi_1,..., \psi_n$; i.e.,

$$({}^a\mathfrak{A})^e = \mathfrak{R}_3\mathscr{S}, \qquad \mathscr{S} = \{f_0, \psi_1,..., \psi_n\}. \tag{14.16}$$

Let Ω be an algebraic closure of the field $\mathbb{C}(\zeta)$,

$$\mathfrak{R}_4 = \Omega[x_2,..., x_n, y_1, y_2]. \tag{14.17}$$

Obviously $\mathfrak{R}_3$ is a subring of $\mathfrak{R}_4$. In this and the next paragraph, we write, for an ideal $\mathfrak{b}$ of $\mathfrak{R}_3$, $\mathfrak{b}^{e'} = \mathfrak{R}_4\mathfrak{b}$, the ideal of $\mathfrak{R}_4$ generated by $\mathfrak{b}$; and write, for an ideal $\mathfrak{B}$ of $\mathfrak{R}_4$, $\mathfrak{B}^{c'} = \mathfrak{B} \cap \mathfrak{R}_3$. For $j \in J$ let $\mathfrak{P}$ $(\subseteq \mathfrak{R}_4)$ be any prime ideal of $({}^a\mathfrak{P}_j)^{ee'}$ $(= (({}^a\mathfrak{P}_j)^e)^{e'}$; some similar notations will be used later on in this paragraph). Then

$$({}^a\mathfrak{A})^{ee'} \subseteq \mathfrak{P}, \tag{14.18}$$

since $({}^a\mathfrak{A})^e \subseteq ({}^a\mathfrak{P}_j)^e$ and $({}^a\mathfrak{P}_j)^{ee'} \subseteq \mathfrak{P}$. Moreover, by [30, Vol. II, pp. 224–225, Theorem 36] and (14.8), we have

$$\mathfrak{P}^{c'} = ({}^a\mathfrak{P}_j)^e, \qquad \operatorname{rank}({}^a\mathfrak{P}_j)^{ee'} = \operatorname{rank}\mathfrak{P} = \operatorname{rank}({}^a\mathfrak{P}_j)^e = n+1. \quad (14.19)$$

Further, we assert that $\mathfrak{P}$ is an isolated prime ideal of $({}^a\mathfrak{A})^{ee'}$. To see this, it suffices to prove, by (14.18) and [30, Vol. I, p. 221, Theorem 7], that if $\mathfrak{P}'$ is any prime ideal of $\mathfrak{R}_4$ satisfying

$$({}^a\mathfrak{A})^{ee'} \subseteq \mathfrak{P}' \subseteq \mathfrak{P} \quad (14.20)$$

then $\mathfrak{P}' = \mathfrak{P}$. Now (14.20) together with (14.19) implies, by [30, Vol. II, p. 221, formula (1)], that

$$({}^a\mathfrak{A})^e = ({}^a\mathfrak{A})^{ee'c'} \subseteq (\mathfrak{P}')^{c'} \subseteq \mathfrak{P}^{c'} = ({}^a\mathfrak{P}_j)^e.$$

This and (14.8) show, by [30, Vol. I, p. 221, Theorem 7], that

$$(\mathfrak{P}')^{c'} = ({}^a\mathfrak{P}_j)^e, \quad (14.21)$$

since $(\mathfrak{P}')^{c'}$ is trivially a prime ideal of $\mathfrak{R}_3 = (\mathfrak{R}_1)_{\mathscr{M}_1}$. By (14.19)–(14.21) and the fact that $(\mathfrak{P}')^{c'e'} \subseteq \mathfrak{P}'$ which is easily verified, we obtain

$$\operatorname{rank}\mathfrak{P} = \operatorname{rank}({}^a\mathfrak{P}_j)^{ee'} = \operatorname{rank}(\mathfrak{P}')^{c'e'} \leqslant \operatorname{rank}\mathfrak{P}' \leqslant \operatorname{rank}\mathfrak{P}.$$

So $\operatorname{rank}\mathfrak{P}' = \operatorname{rank}\mathfrak{P}$. On combining this and (14.20), we conclude that $\mathfrak{P}' = \mathfrak{P}$, and therefore $\mathfrak{P}$ is an isolated prime ideal of $({}^a\mathfrak{A})^{ee'}$ of rank $n+1$, and in addition, $({}^a\mathfrak{A})^{ee'} \neq \mathfrak{R}_4$.

By (14.8) and the above assertion we see that for each $j \in J$, $\mathfrak{P}_j$ corresponds at least one isolated prime ideal of $({}^a\mathfrak{A})^{ee'}$ of rank $n+1$. Furthermore on utilizing (14.19) and the fact that for each $j \in J$ $({}^a\mathfrak{P}_j)^{ec} = {}^a\mathfrak{P}_j$ (by (14.6)), ${}^{ha}\mathfrak{P}_j = \mathfrak{P}_j$ (by (10.10) and the fact that $\mathfrak{P}_j$ is special), it is easily verified that for distinct elements (if any) j_1, j_2 of J, $\mathfrak{P}_{j_1}$ and $\mathfrak{P}_{j_2}$ correspond to distinct isolated prime ideals of $({}^a\mathfrak{A})^{ee'}$ of rank $n+1$. But $({}^a\mathfrak{A})^{ee'} \neq \mathfrak{R}_4$ as remarked above, and

$$({}^a\mathfrak{A})^{ee'} = \mathfrak{R}_4({}^a\mathfrak{A})^e = \mathfrak{R}_4\mathscr{S}$$

by (14.16). So on applying Lemma 12.5 to $\mathfrak{R}_4 = \Omega[x_2, \ldots, x_n, y_1, y_2]$ and the ideal $\mathfrak{R}_4\mathscr{S}$, we see immediately, by (14.16), (14.15), and $2^{n-1}M_0 \geqslant 2$ (since $M \geqslant 2$ by (5.4)), that the cardinal $|J|$ of J, i.e., the number of bad prime ideals of $\mathfrak{I}_n^*$, satisfies

$$|J| \leqslant (n+1)^{n+1}(2L_0)^{n-1} \cdot 3 \cdot 2^{n-1}M_0 = 3 \cdot 4^{n-1}(n+1)^{n+1}L_0^{n-1}M_0.$$

Thus (v) is established.

Now we proceed to prove (i)–(iii) for $r = n + 1$. We first show that for each prime ideal $\mathfrak{P}$ of $\mathfrak{I}_n^*$ there exists some $\boldsymbol{\rho} \in \mathscr{O}_0 = \mathscr{O}^{n+1}(S_0/(n+1),\ldots, s_n/(n+1))$ such that

$$\mathscr{E}(\boldsymbol{\rho})\,\mathfrak{I}_n^* \not\subseteq \mathfrak{P}. \tag{14.22}$$

Suppose that this is false; i.e.,

$$\mathscr{E}(\boldsymbol{\rho})\,\mathfrak{I}_n^* \subseteq \mathfrak{P} \qquad \text{for all } \boldsymbol{\rho} \in \mathscr{O}_0; \tag{14.23}$$

we shall deduce a contradiction. On utilizing (iii) for $r = n$, by some arguments similar to that in Section 13, it is easily seen that $\mathscr{E}(-\boldsymbol{\rho})\mathfrak{P}$ is a prime ideal of $\mathfrak{I}_n^*$ for every $\boldsymbol{\rho} \in \mathscr{O}_0$. We now define an equivalence relation on $\mathbb{Z}_0$ ($\mathbb{Z}_0$ is defined by (13.5)). Recall T is the isomorphism from $\mathbb{Z}^{2(n+1)}$ to $\mathscr{O}^{n+1}$ defined in Section 13. We say that the elements v, v' of $\mathbb{Z}_0$ are equivalent if the elements $\boldsymbol{\rho} = T(v)$, $\boldsymbol{\rho}' = T(v')$ of $\mathscr{O}_0$ satisfy $\mathscr{E}(-\boldsymbol{\rho})\mathfrak{P} = \mathscr{E}(-\boldsymbol{\rho}')\mathfrak{P}$, i.e., $\boldsymbol{\rho}' - \boldsymbol{\rho} \in S(\mathfrak{P})$. Since $\mathscr{E}(-\boldsymbol{\rho})\mathfrak{P}$ is a prime ideal of $\mathfrak{I}_n^*$ for every $\boldsymbol{\rho} \in \mathscr{O}_0$, the number B of equivalence classes does not exceed the total number of prime ideals of $\mathfrak{I}_n^*$. Since $\mathfrak{I}_n^*$ is unmixed (by (iii) for $r = n$ and Lemma 12.2), we have

$$B \leqslant \deg \mathfrak{I}_n^* \leqslant 3 \cdot 4^n (nL_0)^n$$

by (iv) for $r = n$. But the conditions (5.7) and (5.4) imply that

$$\begin{aligned}(S_0/(n+1))^2 \cdots (S_n/(n+1))^2 &\geqslant 3 \cdot 2^n (n+2)^{n+2} L^n M \\ &\geqslant 3 \cdot 4^n (nL_0)^n \geqslant B,\end{aligned}$$

so we can apply Lemma 12.6 with $q = 1$ to $\mathbb{Z}_0$ and the equivalence relation defined above, and see that there exist distinct $\boldsymbol{\rho}$, $\boldsymbol{\rho}'$ in $\mathscr{O}_0$ satisfying $\boldsymbol{\rho}' - \boldsymbol{\rho} \in S(\mathfrak{P})$. According to Lemma 10.3 (2) and Definition 10.1, this shows that $\mathfrak{P}$ is bad prime ideal of $\mathfrak{I}_n^*$. Hence $\mathscr{E}(-\boldsymbol{\rho})\mathfrak{P}$ is a bad prime ideal of $\mathfrak{I}_n^*$ for every $\boldsymbol{\rho} \in \mathscr{O}_0$ by Lemma 10.3 (3) and Definition 10.1. Therefore, the number B of equivalence classes satisfies, by (v), that

$$B \leqslant 3 \cdot 4^{n-1} (n+1)^{n+1} L_0^{n-1} M_0.$$

Now the condition (5.6) enables us to apply Lemma 12.6 with $q = 3$. Hence we see, similarly to Section 13, that rank $S(\mathfrak{P}) \geqslant 3$, i.e.,

$$\text{corank } S(\mathfrak{P}) \leqslant 2n - 1.$$

On the other hand, since $\mathfrak{P}$ is a special homogeneous prime ideal of rank $t + n$, we must have, by (12.7),

$$\text{corank } S(\mathfrak{P}) \geqslant q_n \geqslant 2n.$$

We have thus deduced a contradiction from the falsity of (14.22). This contradiction establishes (14.22). From (14.22), by the similar pattern of arguments as in Section 13, we can construct an adequate homogeneous polynomial P_{t+n+1} and see that (i)–(iii) hold for $r = n+1$.

We now prove (vi). Let

$$\mathfrak{A}_1 = (\mathfrak{G}, P_{t+1},\ldots, P_{t+n+1}).$$

Then $\mathfrak{I}_{n+1} \subseteq \mathfrak{A}_1 \subseteq \mathfrak{I}_{n+1}^*$, so $\mathfrak{I}_{n+1}^* \subseteq \mathfrak{A}_1^* \subseteq (\mathfrak{I}_{n+1}^*)^* = \mathfrak{I}_{n+1}^*$, i.e.,

$$\mathfrak{I}_{n+1}^* = \mathfrak{A}_1^*.$$

From this we see that every prime ideal $\mathfrak{P}$ of $\mathfrak{I}_{n+1}^*$ is an isolated prime ideal of $\mathfrak{A}_1$ of rank $t+n+1$, since $\mathfrak{I}_{n+1}^*$ is unmixed with rank $t+n+1$ (by (iii) for $r = n+1$ and Lemma 12.2) and $\mathfrak{P} \cap \mathscr{M} = \varnothing$. As in the proof of (v), we see that ${}^a\mathfrak{P}$ is an isolated prime ideal of ${}^a\mathfrak{A}_1$. By $\mathfrak{S} \subseteq \mathfrak{G} \subseteq \mathfrak{P}$ and $Z_{00} \notin \mathfrak{P}$, Lemma 10.1 (7) implies that

$$\operatorname{rank} {}^a\mathfrak{P} = \operatorname{rank} \mathfrak{P} - 2n = t + n + 1 - 2n = n + 2.$$

So ${}^a\mathfrak{P} \neq \mathfrak{R}_1$, whence ${}^a\mathfrak{A}_1 \neq \mathfrak{R}_1$ since ${}^a\mathfrak{A}_1 \subseteq {}^a\mathfrak{P}$. Furthermore if $\mathfrak{P} \neq \mathfrak{P}'$ are any prime ideals of $\mathfrak{I}_{n+1}^*$ then ${}^a\mathfrak{P} \neq {}^a\mathfrak{P}'$ by (10.10) and the fact that $Z_{00} \notin \mathfrak{P}$, $Z_{00} \notin \mathfrak{P}'$. Thus we conclude that the number of prime ideals of $\mathfrak{I}_{n+1}^*$ does not exceed the number of isolated prime ideals of ${}^a\mathfrak{A}_1$ of rank $n+2$. Now by (12.3), (i) for $r = n+1$, Lemma 12.4, we see that

$$\begin{aligned} {}^a\mathfrak{A}_1 &= (f_0, {}^aP_{t+1},\ldots, {}^aP_{t+n+1}) \\ &= (f_0, f_1,\ldots, f_{n+1}), \end{aligned} \tag{14.24}$$

where $f_0 = y_2^2 - 4y_1^3 + g_2 y_1 + g_3$, $f_1,\ldots, f_n$ are the polynomials in $\mathfrak{R}_1$ satisfying (14.11) and (14.12), and $f_{n+1} \in \mathfrak{R}_1$ satisfies ${}^aP_{t+n+1} \equiv f_{n+1} \pmod{f_0}$ and the conditions

$$\deg_{x_l} f_{n+1} \leqslant L_0 \ (1 \leqslant l \leqslant n), \quad \deg_{y_1} f_{n+1} \leqslant 2, \quad \deg_{y_2} f_{n+1} \leqslant 2^n M_0. \tag{14.25}$$

On applying Lemma 12.5 to $\mathfrak{R}_1 = \mathbb{C}[x_1,\ldots, x_n, y_1, y_2]$ and the ideal ${}^a\mathfrak{A}_1 = (f_0, f_1,\ldots, f_{n+1})$ and utilizing (14.12), (14.25), $2^n M_0 \geqslant 2$ (since $M \geqslant 2$ by (5.4)), (vi) follows immediately.

To complete the proof of the Inductive Lemma it remains only to verify (ii), (iii), for $r = n+2$. Arguing as before, on combining (vi), (5.7), Lemma 12.6 with $q = 1$ and the fact that $q_{n+1} = 2(n+1)$ (by (12.7)), we see that for each prime ideal $\mathfrak{P}$ of $\mathfrak{I}_{n+1}^*$ there exists some $\boldsymbol{\rho} \in \mathscr{O}_0$ such that

$$\mathscr{E}(\boldsymbol{\rho})\, \mathfrak{I}_{n+1}^* \not\subseteq \mathfrak{P}. \tag{14.26}$$

As in Section 13, it is easily seen from (14.26) that

$$E(\rho)P_{t+i} \notin \mathfrak{P}$$

for some i with $1 \leqslant i \leqslant n+1$. Set $Q_{\mathfrak{P}} = E(\rho)P_{t+i}$. By [10, Lemma 5] there exists $\lambda_{\mathfrak{P}} \in \mathbb{C}$ for each $\mathfrak{P}$ such that

$$P_{t+n+2} = \sum \lambda_{\mathfrak{P}} Q_{\mathfrak{P}} \notin \mathfrak{P}'$$

for any prime ideal $\mathfrak{P}'$ of $\mathfrak{I}^*_{n+1}$, where the sum is taken over all prime ideals $\mathfrak{P}$ of $\mathfrak{I}^*_{n+1}$. Now it is readily verified that (ii) and (iii) hold for $r = n+2$. This completes the proof of the Inductive Lemma.

Proof of Proposition 5.1 (*Completion*). From the falsity of Proposition 5.1, we have, by the Inductive Lemma, constructed the ideal $\mathfrak{I}^*_{n+2}$. This is a homogeneous ideal of $\mathfrak{R} = \mathbb{C}[Z_{00},..., \mathbb{Z}_{n2}]$ of rank $t+n+2 = N+1$. Since there is only a single homogeneous prime ideal $\mathfrak{M} = (Z_{00},..., Z_{n2})$ of $\mathfrak{R}$ of rank $N+1$, the ideal $\mathfrak{I}^*_{n+2}$ must be primary with $\sqrt{\mathfrak{I}^*_{n+2}} = \mathfrak{M}$. This implies that $\mathfrak{I}^*_{n+2}$ has no zeroes on $\mathbb{P}^N$, so in particular none on Γ. Hence $\mathfrak{I}_{n+2}$ has no zeroes on Γ, which contradicts the fact that $\mathfrak{I}_{n+2}$ vanishes on $\Gamma_{n+1} = \{(0,..., 0) \times \psi(0)\} \subseteq \Gamma$ (see the Inductive Lemma, (ii) for $r = n+2$). This contradiction proves Proposition 5.1.

On recalling the remark at the beginning of Section 9, the proofs of Theorem 1′, Theorem 1, and its Corollary are complete.

APPENDIX: Proof of Lemma 12.5

We start with a general remark. Let $\mathfrak{I}$, $\mathfrak{P}$ be arbitrary non-zero proper ideals of a commutative noetherian ring $\mathfrak{R}$, with $\mathfrak{P}$ prime. Then a necessary and sufficient condition that $\mathfrak{P}$ should be an isolated prime ideal of $\mathfrak{I}$ is that there should exist an integer $e \geqslant 1$ and an element α of $\mathfrak{R}$ not in $\mathfrak{P}$ such that

$$\alpha\mathfrak{P}^e \subseteq \mathfrak{I} \subseteq \mathfrak{P}. \tag{A.1}$$

For let

$$\mathfrak{I} = \mathfrak{Q}_0 \cap \cdots \cap \mathfrak{Q}_m \qquad (\sqrt{\mathfrak{Q}_i} = \mathfrak{P}_i \quad (0 \leqslant i \leqslant m)) \tag{A.2}$$

be an irredundant primary representation with exponents $e_0,..., e_m$ (i.e., e_i is the least positive integer such that $\mathfrak{P}_i^{e_i} \subseteq \mathfrak{Q}_i$). For the necessity we may suppose that $\mathfrak{P} = \mathfrak{P}_0$ is isolated; then it is minimal among $\mathfrak{P}_0,..., \mathfrak{P}_m$ and so we can select α_i in $\mathfrak{P}_i$ not in $\mathfrak{P}_0$ $(1 \leqslant i \leqslant m)$. Now (A.1) follows with $\alpha = \alpha_1^{e_1} \cdots \alpha_m^{e_m}$ and $e = e_0$. For the sufficiency we observe that the right-hand inclusion of (A.1) implies that at least one of the prime ideals $\mathfrak{P}_0,..., \mathfrak{P}_m$ is

contained in $\mathfrak{P}$; we may suppose that $\mathfrak{P}_0 \subseteq \mathfrak{P}$ and that $\mathfrak{P}_0$ is minimal among such prime ideals contained in $\mathfrak{P}$. Then clearly $\mathfrak{P}_0$ is minimal among $\mathfrak{P}_0,\ldots,\mathfrak{P}_m$, and hence it is an isolated prime ideal of $\mathfrak{I}$. Now the left-hand inclusion of (A.1) leads to $\alpha\mathfrak{P}^e \subseteq \mathfrak{P}_0$, and as α is not in $\mathfrak{P}$, it is not in $\mathfrak{P}_0$, whence $\mathfrak{P} \subseteq \mathfrak{P}_0$. Thus $\mathfrak{P} = \mathfrak{P}_0$. This establishes our opening remark.

To continue the proof we fix elements $\theta_1,\ldots,\theta_n$ of Ω such that

$$\theta_i \neq \xi_i \qquad (1 \leqslant i \leqslant n) \tag{A.3}$$

for every isolated prime ideal $(x_1-\xi_1,\ldots,x_n-\xi_n)$ of $\mathfrak{I} = (P_1,\ldots,P_l)$ of rank n. Put $E = D_1 \cdots D_n$, $E_i = E/D_i$ $(1 \leqslant i \leqslant n)$ and

$$Q_j(y_1,\ldots,y_n) = P_j(y_1^{E_1}+\theta_1,\ldots,y_n^{E_n}+\theta_n) \qquad (1 \leqslant j \leqslant l). \tag{A.4}$$

If $(x_1-\xi_1,\ldots,x_n-\xi_n)$ is an isolated prime ideal of $\mathfrak{I}$ of rank n and $\eta_1,\ldots,\eta_n$ are any elements of Ω satisfying

$$\eta_i^{E_i}+\theta_i = \xi_i \qquad (1 \leqslant i \leqslant n) \tag{A.5}$$

we proceed to show that $(y_1-\eta_1,\ldots,y_n-\eta_n)$ is an isolated prime ideal of $\mathfrak{I} = (Q_1,\ldots,Q_l)$ of rank n in $\Omega[y_1,\ldots,y_n]$.

This is geometrically obvious, but we can argue algebraically as follows. By our opening remark we can find an integer $e \geqslant 1$ and a polynomial $A(x_1,\ldots,x_n)$ in $\Omega[x_1,\ldots,x_n]$ with $A(\xi_1,\ldots,\xi_n) \neq 0$ such that $\mathfrak{I}$ lies in $(x_1-\xi_1,\ldots,x_n-\xi_n)$ and contains $A(x_1,\ldots,x_n)\cdot(x_i-\xi_i)^e$ $(1 \leqslant i \leqslant n)$. Replacing x_i by $y_i^{E_i}+\theta_i$ $(1 \leqslant i \leqslant n)$, we see from (A.4) and (A.5) that $\mathfrak{I}$ lies in $(y_1^{E_1}-\eta_1^{E_1},\ldots,y_n^{E_n}-\eta_n^{E_n}) \subseteq (y_1-\eta_1,\ldots,y_n-\eta_n)$ and contains $B_0(y_1,\ldots,y_n)(y_i^{E_i}-\eta_i^{E_i})^e$ $(1 \leqslant i \leqslant n)$, where

$$B_0(y_1,\ldots,y_n) = A(y_1^{E_1}+\theta_1,\ldots,y_n^{E_n}+\theta_n).$$

Here $B_0(\eta_1,\ldots,\eta_n) = A(\xi_1,\ldots,\xi_n) \neq 0$ by (A.5). Hence $\mathfrak{I}$ contains $B(y_1,\ldots,y_n)(y_i-\eta_i)^e$ $(1 \leqslant i \leqslant n)$, where

$$B(y_1,\ldots,y_n) = B_0(y_1,\ldots,y_n)\prod_{i=1}^{n}\left(\frac{y_i^{E_i}-\eta_i^{E_i}}{y_i-\eta_i}\right)^e.$$

Now

$$B(\eta_1,\ldots,\eta_n) = B_0(\eta_1,\ldots,\eta_n)\prod_{i=1}^{n}(E_i\eta_i^{E_i-1})^e$$

and by (A.3) and (A.5) we have $\eta_i \neq 0$ $(1 \leqslant i \leqslant n)$; hence $B(\eta_1,\ldots,\eta_n) \neq 0$. Thus by our opening remark $(y_1-\eta_1,\ldots,y_n-\eta_n)$ is indeed an isolated prime ideal of $\mathfrak{I}$, since $(y_1-\eta_1,\ldots,y_n-\eta_n)^f \subseteq ((y_1-\eta_1)^e,\ldots,(y_n-\eta_n)^e)$ for $f = n(e-1)+1$.

Now suppose there are exactly $N \geqslant 1$ isolated prime ideals $(x_1 - \xi_1, ..., x_n - \xi_n)$ of $\mathfrak{I} = (P_1, ..., P_l)$ of rank n. By selecting all roots of (A.5) and using (A.3) we see that each of these gives rise to $E_1 \cdots E_n = E^{n-1}$ different isolated prime ideals $(y_1 - \eta_1, ..., y_n - \eta_n)$ of $\mathfrak{I} = (Q_1, ..., Q_l)$ of rank n. Plainly the resulting NE^{n-1} such ideals are all different. But the polynomials $Q_1, ..., Q_l$ have total degrees at most $D_1E_1 + \cdots + D_nE_n = nE$ by (A.4), and hence by the Corollary in [23, Sect. 2] (we remark that the results of [23, Sect. 2] are valid for arbitrary fields K being algebraically closed and of characteristic 0) we must have $NE^{n-1} \leqslant (nE)^n$. Therefore $N \leqslant n^nE = n^nD_1 \cdots D_n$, which establishes Lemma 12.5.

ACKNOWLEDGMENTS

Most of the work for this paper was done while the author was enjoying the hospitality of the Institut Henri Poincaré and the University of Nottingham in 1981, and the main results were reported on in the Journées Arithmétiques, Metz, France, 1981. The author would like to express his warmest gratitude to David Masser and Michel Waldschmidt for suggesting the problem. The general idea of dividing the prime ideals of a given ideal into good and bad ones, and of dehomogenizing, was suggested by David Masser; Michel Waldschmidt suggested using his interpolation method in several variables to construct auxiliary functions. Ultimately, the work owes its existence to their constant advice and encouragement.

REFERENCES

1. M. ANDERSON, Inhomogeneous linear forms in algebraic points of an elliptic function, *in* "Transcendence Theory: Advances and Applications" (A. Baker and D. W. Masser, Eds.), pp. 121–143, Academic Press, London/New York, 1977.
2. M. ANDERSON, "Linear Forms in Algebraic Points of an Elliptic Function," Ph. D. thesis, University of Nottingham, 1978.
3. M. ANDERSON AND D. W. MASSER, Lower bounds for heights on elliptic curves, *Math. Z.* **174** (1980), 23–34.
4. A. BAKER, On the periods of the Weierstrass $\wp$-function, *in* "Symposia Math. IV. INDAM Roma, 1968," pp. 155–174. Academic Press, London, 1970.
5. A. BAKER, The theory of linear forms in logarithms, *in* "Transcendence Theory: Advances and Applications" (A. Baker and D. W. Masser, Eds.), pp. 1–27, Academic Press, London/New York, 1977.
6. M. BASHMAKOV, Un théorème de finitude sur la cohomologie des courbes elliptiques, *C. R. Acad. Sci. Paris Ser. I Math.* **270** (1970), 999–1001.
7. D. BERTRAND, Approximations diophantiennes p-adiques sur les courbes elliptiques admettant une multiplication complexe, *Compositio Math.* **37** (1978), 21–50.
8. D. BERTRAND AND D. W. MASSER, Linear forms in elliptic integrals, *Invent. Math.* **58** (1980), 283–288.
9. A. BOREL, "Linear Algebraic Groups," Benjamin, New York, 1969.
10. W. D. BROWNAWELL AND D. W. MASSER, Multiplicity estimates for analytic functions II, *Duke Math. J.* **47** (1980), 273–295.

11. G. V. CHUDNOVSKY, Algebraic independence of values of exponential and elliptic functions, *in* "Proceedings, International Congress of Mathematicians, Helsinki, 1978," Vol. 1, pp. 339–350.
12. H. GROSCOT, Points entiers sur les courbes elliptiques, *C. R. Acad. Sci. Paris Ser. I Math.* **292** (1981), 859–862.
13. R. HARTSHORNE, "Algebraic Geometry," Springer-Verlag, New York/Heidelberg/Berlin, 1977.
14. W. V. D. HODGE AND D. PEDOE, "Methods of Algebraic Geometry," Vol. II, Cambridge Univ. Press, Cambridge, 1952.
15. E. R. KOLCHIN, Algebraic groups and algebraic dependence, *Amer. J. Math.* **90** (1968), 1151–1164.
16. S. LANG, "Elliptic Curves, Diophantine Analysis," Springer-Verlag, Berlin/Heidelberg/New York, 1978.
17. M. LAURENT, Minoration de la hauteur de Néron-Tate, *in* "Sém. Théorie des Nombres Paris, 1981/1982," Ser. Progress in Math., Birkhäuser-Verlag, Basel, 1983.
18. K. MAHLER, On some inequalities for polynomials in several variables, *J. London Math. Soc.* **37** (1962), 341–344.
19. D. W. MASSER, "Elliptic Functions and Transcendence," Lecture Notes in Mathematics No. 437, Springer-Verlag, Berlin, 1975.
20. D. W. MASSER, Division fields of elliptic functions, *Bull. London Math. Soc.* **9** (1977), 49–53.
21. D. W. MASSER, On polynomials and exponential polynomials in several complex variables, *Invent. Math.* **63** (1981), 81–95.
22. D. W. MASSER AND G. WÜSTHOLZ, Zero estimates on group varieties I, *Invent. Math.* **64** (1981), 489–516.
23. D. W. MASSER AND G. WÜSTHOLZ, Fields of large transcendence degree generated by values of elliptic functions, *Invent. Math.*, in press.
24. M. MIGNOTTE AND M. WALDSCHMIDT, Linear forms in two logarithms and Schneider's method, *Math. Ann.* **231** (1978), 241–267.
25. M. WALDSCHMIDT, A lower bound for linear forms in logarithms, *Acta Arith.* **37** (1980), 257–283.
26. M. WALDSCHMIDT, Transcendance et exponentielles en plusieurs variables, *Invent. Math.* **63** (1981), 97–127.
27. H. WEYL, "Algebraic Theory of Numbers," Princeton Univ. Press, Princeton, N. J., 1940.
28. E. T. WHITTAKER AND G. N. WATSON, "A Course of Modern Analysis," Cambridge Univ. Press, Cambridge, 1965.
29. KUNRUI YU, Special linear forms in elliptic logarithms, to appear.
30. O. ZARISKI AND P. SAMUEL, "Commutative Algebra," Springer-Verlag, New York, 1979.
31. H. G. ZIMMER, On the difference of the Weil height and the Néron–Tate height, *Math. Z.* **147** (1976), 35–51.